

[Ed. Note: Due to the rapidly changing nature of this area of law, some of the content in this paper may be outdated, and should not be relied upon for legal research or citation.]

SECURITY SOFTWARE: IS THERE A “FIREWALL” SHIELDING MANUFACTURERS
FROM TORT LIABILITY?

Kevin S. Brady

I.	INTRODUCTION	1
II.	A PRIMER ON SECURITY SOFTWARE	5
III.	PRODUCTS LIABILITY CONCEPTS	6
	A. Strict Liability	7
	B. Negligence	8
	C. Breach of Warranty	9
	D. Types of Defects	10
	E. Causation	11
	F. Disclaimers and Limitations of Remedies	12
IV.	LIABILITY EXTENDING TO SOFTWARE VENDORS	13
	A. Development of Software Products Liability	14
	B. Burglar and Fire Alarms: Analogous Case Law That May Have a Bearing on Software Liability	20
	C. Fact Patterns That Conceivably Give Rise to Liability	22
	1. Liability Arising From Personal Physical Injury	25
	2. Liability Arising From Invasion of Privacy	28
V.	CONCLUSION	32

I. INTRODUCTION

Imagine a scenario where a malicious person, a hacker, gains entry into a secured computer system used by an online retailer. This person proceeds to acquire the credit card information, including the identities, of thousands of the online retailer's customers. Imagine other scenarios where a malfeasant similarly gains access to patient medical data such as HIV or abortion records from the computer database of a medical institution, proprietary customer data from a financial institution, trade secret information from a corporation, or sensitive client information from a law firm. Imagine yet another situation where a hacker gains access to personal data residing on a private individual's home PC. Now imagine that this unlawfully acquired data becomes posted on the Internet, or is turned over to other malevolent parties. It requires little stretch of the imagination to envision the high degree of damage that would quickly occur, not only to the parties on the receiving end of the intrusion, but to numerous third party victims as well. These types of situations can and do occur, due largely to the vulnerabilities of computer networks coupled with the increasing sophistication and elusiveness of computer hackers. The required protection scheme becomes one analogous to protecting premises from burglars. As with the prevention of burglaries, there are security systems that can be employed to minimize the risk of damage from computer intrusions. Such systems are intended to protect valuable data assets, much like locks and burglar alarms protect physical assets, but they are by no means infallible.

The rise of the Internet in the past decade has resulted in a system wherein vast numbers of organizations have placed chosen information about their products, services, customers, and

other data within easy reach of the online masses. The widespread implementation of local computer network systems in recent years has enabled organizations to easily manage their internal data. Unfortunately, these two trends have collided: organizations may find themselves within easy reach of persons whose goals are to use the Internet to penetrate their internal computer systems to obtain far more sensitive information and to create great harm to the organizations.¹ Computer hackers now maliciously gain access to proprietary content within organizations' computer systems, or introduce computer viruses or worms into those systems.²

In recent years, actions taken by some hackers against online entities have become far more sophisticated and notorious. Many of these hackers have clear agendas: social/political activism, economic gain, or espionage. Others hack merely for their own amusement. Activist hackers have cracked into computer systems, causing damage to the systems or defacing websites by leaving propaganda for other online visitors to see.³ Other malicious parties have hacked into systems to obtain data in an effort to extort money from the rightful owners of the data. For example, in January 2000, approximately 350,000 credit card numbers were stolen from the online music retailer CD Universe. The hacker held the credit card information "hostage," demanding payment of \$100,000. When the company refused, the hacker posted the credit card numbers on

¹ Computer security vulnerabilities have more than doubled in one year, increasing from a reported 1,090 holes in 2000, to 2,437 holes in 2001. In addition, the number of reported security incidents increased from 21,756 in 2000 to 52,658 in 2001. <http://www.cert.org/stats/cert_stats.html>

² In 2001, the estimated worldwide impact of malicious computer code, such as computer viruses, was 13.2 billion dollars. <<http://www.computereconomics.com/cei/press/pr92101.htm>>

³ In the week of May 1, 2001, a computer virus called the "sadmind/IIS worm," was believed to have infected 8,836 computer servers. This virus instructed those systems to leave a defacement message containing an inflammatory statement about the United States government and a "calling card" in China. <<http://www.attrition.org/security/commentary/worm01.html>>

an Internet web site. This caused problems not only for the online retailer, but also for the credit card companies who were subsequently forced to cancel and reissue those credit card accounts, typically at a cost to the credit card company of \$5 to \$25 per card.⁴ Hacking has been used to unlawfully obtain trade secrets or other sensitive information from businesses and governmental agencies.⁵

The vast majority of these hacker intrusions into organizations' computer systems can be prevented through vigilance by the information technology (IT) professionals who oversee the operations of these systems.⁶ However, despite these reasonable efforts on the part of computer professionals, a closer look must be made into unlawful intrusions that occur despite the diligence of the user. Thus, attention must be given to potential liability arising from intrusions that are enabled by defects in the security software relied upon by the user. If hacker intrusions occur due to software flaws and property damage or personal injury is suffered by the user, the question then becomes whether tort law provides remedies to the user and other injured parties.

This paper will analyze these questions to determine what fact patterns might give rise to products liability actions against those engaged in the development, manufacturing and distribution of such software. Theories of liability will be examined for harms including property damage, personal injury, and injury due to invasions of privacy.

⁴ GREG SANDOVAL, *War on Cybercrime – We're Losing*, ZDNet News, May 14, 2002. <<http://www.zdnet.com.com/2102-1106-912780.html>>

⁵ It was reported that approximately 25,000 attempted intrusions were made into United States defense computer systems in 2000. Of those attempts, 245 were successful. <http://www.gcn.com/vol1_no1/daily-updates/4028-1.html>

⁶ Of the 245 successful intrusions made against U.S. defense computer systems in 2000, officials determined that 96 percent of those intrusions could have been prevented if users had followed protocols. *Id.*

II. A PRIMER ON SECURITY SOFTWARE

Organizations that maintain an online presence generally protect their computer systems by means of security software, commonly with what is known as a “firewall” computer program. The firewall computer program is the software component of a firewall system. A firewall system is defined as “a single point between two or more networks (a) through which all traffic must pass, (b) with which traffic can be controlled and often authenticated, and (c) in which all traffic is logged.”⁷ A firewall computer program is typically installed on a “firewall machine,” a dedicated gateway computer used to protect a cluster of more loosely administered machines (often the user’s internal network) hidden behind it.⁸ The manner in which these firewall programs are relied upon to protect a computer system from unauthorized access is analogous to a guard desk at the entrance to a building. The guard desk is located at a control point, with the guard on duty allowing authorized persons to pass within while keeping out unauthorized persons. The guard may check the identities of persons passing through the control point, inspect the contents of carried items, and monitor the movement of visitors within the building. Similarly, the firewall program allows the free flow of authorized data traffic while blocking out unwanted traffic. Like the building’s guard, the firewall program can be used to track the identity of data traffic and log its movement. The firewall may employ special precautions, such as threat monitoring, “callback” authentication features where a system administrator is alerted of unauthorized access

⁷ BILL CHESWICK & STEVE BELLOVIN, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley 1994.

⁸ Definition of “firewall machine.” DENIS HOWE, FREE ON-LINE DICTIONARY OF COMPUTING (FOLDOC). <<http://www.foldoc.org>>

attempts⁹, and “iron box” systems to set traps for identifying potential hackers.¹⁰ Another function of a firewall program is to encrypt data traffic between connections in a virtual private network (VPN). A VPN is a secure connection between users through an otherwise insecure network such as the Internet, allowing a less costly alternative to using dedicated private lines.¹¹ The firewall program is designed to prevent unauthorized access to data being transferred across the VPN.

III. PRODUCTS LIABILITY CONCEPTS

There are three primary theories in products liability that will be examined as possible means of recovery in cases involving software. These theories are: 1) strict liability in tort; 2) negligence liability in tort; and 3) breach of warranty. Types of product defects must also be examined, as the theory of recovery will turn on the nature of the defect alleged. In addition, one must analyze the causation between the defect and the manufacturer’s conduct associated with that defect, and the damages incurred by the plaintiff. Finally, attention must be given to disclaimers, as these are commonly employed in sales agreements involving software and related

⁹ Definition of “callback.” A “callback” feature is used by some dial-up systems to identify a user who is attempting to access the system. When a user attempts to log in to the system, the callback feature dials up the user’s registered telephone number to confirm. If an unauthorized user discovers the password to the system, the callback will be sent, not to the unauthorized user, but to the authorized one, and thus alerting the system operator of an attack. *Id.*

¹⁰ Definition of “iron box.” An “iron box” system is a feature designed to trap a potential hacker by placing “bait files” of useless but intriguing data to keep him interested and logged on, allowing time for his identity or source to be determined. *Id.*

¹¹ Definition of “virtual private network.” *Id.*

systems, and may form an affirmative defense to a products liability action.

A. Strict Liability

Strict liability holds a defendant liable for harm to a plaintiff despite the reasonableness of the defendant's actions. The plaintiff is not required to be in direct privity with the defendant, nor is the plaintiff required to maintain a traditional negligence or warranty action.¹² Thus, a manufacturer of a product can be found liable even though the manufacturer had exhausted all reasonable avenues of quality control. Strict liability looks at the product, not the conduct of the defendant.¹³

The application of strict liability to products is generally confined to harms caused by a manufacturing defect in a product.¹⁴ Strict liability without fault is intended to place responsibility for damage caused by defective goods to the manufacturer, a party better positioned to bear that burden. Strict liability also enables plaintiffs, often consumers, to overcome what would ordinarily be a difficult if not insurmountable burden of proof. Strict liability therefore operates much like the theory of *res ipsa loquitur*.¹⁵

There has been some commentary during the past two decades suggesting that strict

¹² RESTATEMENT THIRD, TORTS: PRODUCTS LIABILITY § 1 cmt. a. (1998).

¹³ *Greenman v. Yuba Power Products, Inc.*, 59 Cal.2d 57 (1963).

¹⁴ RESTATEMENT, *supra* note 12, § 2 sub. (a).

¹⁵ *Id.*

liability should attach in cases of software defects resulting in harm to property,¹⁶ however the case law to date has largely failed to develop into those areas.¹⁷ As of this writing, there are no cases on point applying strict liability to software defects.¹⁸

B. Negligence

Negligence is conduct that falls below the legal standard for protecting others against unreasonable risk of harm, that which is a “departure from the conduct expected of a reasonably prudent man under like circumstances.”¹⁹ A company that holds itself out as being capable in its business, impliedly represents that it will perform its work with the “diligence ordinarily possessed by well-informed members of the trade or profession.”²⁰

The theory of negligence is based on the classic “reasonable person” test. Four elements are required to show negligence: 1) a duty of reasonable care, recognized by the law, owed by the defendant; 2) a breach of that duty; 3) a reasonably close causal connection between the defendant’s conduct and the resulting injury; and 4) an actual loss or damage to the interests of

¹⁶ See, e.g., ROBERT D. SPRAGUE, SOFTWARE PRODUCTS LIABILITY: HAS ITS TIME ARRIVED?, 19 W. St. U. L. Rev. 137 (1991), proposing not only that physical injuries caused by defective software should “clearly be recoverable” under a strict products liability claim, but also that a strict liability action for destruction of tangible property “should be successful.” *Id.* at 153.

¹⁷ RESTATEMENT, *supra* note 12, § 19 cmt. d.

¹⁸ *Id.*

¹⁹ MICHAEL RUSTAD & LORI E. EISENSCHMIDT, THE COMMERCIAL LAW OF INTERNET SECURITY, 10 High Tech. L. J. 213 (1995) (citing *Pence v. Ketchum*, 326 So. 2d 831, 835 (La. 1976)).

²⁰ *Id.* (Citing *Data Processing Services, Inc. v. L.H. Smith Oil Co.*, 492 N.E.2d 314, 319 (Ind. Ct. App. 1986)).

another.²¹ Harms caused by defects in the design of a product or inadequate instructions or warnings are typical defects that may trigger a claim for negligence.²²

C. Breach of Warranty

Article 2 of the Uniform Commercial Code (UCC) governs in breach of warranty claims. Causes of actions under breach of warranty can be divided into three different theories: 1) implied warranty of merchantability; 2) implied warranty of fitness for a particular purpose; and 3) express warranty.²³ The first two warranty theories, noted *supra*, are warranties of quality. The first theory is a warranty that the goods are of merchantable quality when they are bought from one who deals in goods of that description. The second theory is a warranty that the goods are fit for the particular purpose of the buyer, when that purpose is made known to the seller and the latter knows that the buyer is relying upon his skill and judgment to select and furnish suitable goods.²⁴ The third theory is express warranty. A seller creates an express warranty when the seller makes to the buyer, as part of the basis of the bargain, any affirmation or promise relating to the goods, any description of the goods, or any sample or model.²⁵ For instance, language contained in

²¹ W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 30 at 164 (5th ed. 1984).

²² RESTATEMENT, *supra* note 12, § 2 sub. (a), (b). *See also*, MacPherson v. Buick Motor Co., 217 N.Y. 382 (1916), where Judge Cardozo, writing the court's opinion, "If [the manufacturer] is negligent where danger is to be foreseen, a liability will follow." MacPherson thus became the pioneering case establishing the application of negligence law to a product.

²³ U.C.C. ART. II, §§ 313-315.

²⁴ KEETON, *supra* note 21, § 95A at 681.

²⁵ U.C.C. ART. II, § 313.

documentation accompanying a software program can create an express warranty.

D. Types of Defects

The Restatement deems a product defective “when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instruction or warnings.”²⁶ A manufacturing defect occurs when the product departs from its intended design, despite all possible care exercised in the preparation and marketing of the product.²⁷ The product defect “may be caused by the way it was manufactured, assembled, inspected, packaged, [or] tested.”²⁸

Defects found in software programs, commonly referred to as “bugs,” can be defined as defects which if not removed would cause a program or system to fail or to produce incorrect results.²⁹ A software defect is a “material breach” of the contract for sale or license of the software if it is so serious that the customer can justifiably demand a fix or can cancel the contract, return the software, and demand a refund.³⁰

It has been held that a product defect can be inferred without proof of a specific defect. If

²⁶ RESTATEMENT, *supra* note 12, § 2.

²⁷ *Id.*, § 2(a).

²⁸ Minnesota civil jury instructions concerning manufacturing defects in products liability cases, MNPRAC CIVJIG 75.30 (4th ed. 1999).

²⁹ CAPERS JONES, APPLIED SOFTWARE MEASUREMENT 273 (1991), *quoted in* CEM KANER, WHAT IS A SERIOUS BUG? DEFINING A “MATERIAL BREACH” OF A SOFTWARE LICENSE AGREEMENT (1996).
<<http://www.badsoftware.com/uccdefect.htm>>

³⁰ KANER, *supra* note 29.

the incident was of a kind that ordinarily occurs as a result of product defect, and was not solely the result of other causes, it may be inferred that the harm was caused by a defect existing at the time of sale or distribution.³¹

E. Causation

Whether a product defect caused harm to persons or property is determined by the prevailing rules and principles governing causation in tort.³² There are no special rules of causation for products liability cases; the rules governing tort law in general apply.³³ There must be “some reasonable connection between the act or omission of the defendant and the damage which the plaintiff has suffered.”³⁴

The ultimate goal of security software is to prevent unauthorized entry into computer systems. Since this software is designed for this specific purpose, it follows that an unauthorized intrusion would be viewed as a foreseeable intervening cause. If an intervening act is one that a defendant has reason to anticipate under particular circumstances, the defendant may be negligent

³¹ RESTATEMENT, *supra* note 12, § 3. *See also* Rector v. Michigan Security Systems, Inc., 407 Mich. 864 (1979). The Michigan Supreme Court reversed an appeals court judgment affirming a jury verdict of no cause of action and remanded for retrial for reasons stated by the dissenting appeals court judge in Rector v. Michigan Security Systems, Inc., 90 Mich. App. 291 (1979), *revd.* 407 Mich. 864. It was held that the plaintiff’s evidence allowed the inference that some defect was present, and that the plaintiff would have sustained her burden in showing a defect attributable to the company if she established a reasonable probability that the defect was attributable to the company.

³² RESTATEMENT, *supra* note 12, § 15.

³³ *See Id.*, *cmt. a.*

³⁴ KEETON, *supra* note 21, § 41 at 263.

for failing to guard against it.³⁵ The courts are in strong agreement that a foreseeable intervening cause will not supersede a defendant's responsibility.³⁶

F. Disclaimers and Limitations of Remedies

Disclaimers and other contractual limitations of remedies by sellers or distributors of new products that attempt to avoid or limit liability for harm to persons are void.³⁷ The public policy argument behind this rule is that the ordinary product user lacks sufficient bargaining power to enter into an agreement limiting his rights to recover.³⁸

Under a strong majority of courts, remedies for harms to the defective product itself are confined to the purview of the Uniform Commercial Code (UCC), often under an implied warranty of merchantability.³⁹ This concept, known as the "economic loss doctrine," promotes the view that damages for economic loss sound in contract, not in tort. Courts focus on the nature of the defect and examine whether the product created a dangerous situation resulting in injury to persons or other property, or just to the product itself.⁴⁰ The latter type of loss is the

³⁵ *Id.*, § 44 at 303.

³⁶ *Id.*

³⁷ RESTATEMENT, *supra* note 12, § 18 cmt. a. *See also* Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960), holding that the Uniform Sales Act "did not authorize the automobile manufacturer to use its grossly disproportionate bargaining power to relieve itself from liability ..."

³⁸ *Id.*

³⁹ U.C.C. ART. II, § 314.

⁴⁰ The leading case setting forth this distinction is *East River Steamship Corp. v. Transamerica Deleva, Inc.*, 476 U.S. 858 (1986), holding that economic loss to the product itself is a remedy sounding in contract and not

diminution in the value of the product due to its inferiority in quality and its failure to work properly for its intended purpose. Such losses are commonly viewed as little more than disappointed expectations,⁴¹ and are commonly bargained for in contractual limitations of liability. Such contractual limitations, when fairly bargained for, often provide an effective means for parties to allocate risks of economic harm between themselves.⁴²

Disclaimers and limitations of remedies for damage to property other than the product itself have become the subject of much litigation and controversy in recent years. The Restatement has not addressed the question of whether this area falls under the purview of tort law, and has left the issue to developing case law.⁴³ However, this case law has demonstrated that disclaimer terms set forth in an agreement will usually be held valid,⁴⁴ unless the defendant's conduct rises to the level of gross negligence, or an intentional tort, such as fraud or misrepresentation.⁴⁵

IV. LIABILITY EXTENDING TO SOFTWARE VENDORS

in tort. While confining economic "product loss" remedies to provisions set forth in the U.C.C., East River did not place limitations on possible tort remedies for damages suffered to property other than the product itself.

⁴¹ *Moorman Manufacturing Co. v. National Tank Co.*, 91 Ill.2d 69 (1982).

⁴² RESTATEMENT, *supra* note 12, § 21 cmt. f.

⁴³ *Id.*

⁴⁴ MARTIN J. McMAHON, LIABILITY OF PERSON FURNISHING, INSTALLING, OR SERVICING BURGLARY OR FIRE ALARM SYSTEM FOR BURGLARY OR FIRE LOSS, 37 A.L.R. 4th 47 (2002).

⁴⁵ *See, e.g., Mankap Enterprises, Inc. v. Wells Fargo Alarm Services*, 427 So. 2d 332 (Fla. App. 1983) (summary judgment affirmed in favor of defendant burglar alarm company as to counts based on alleged negligence and the unconscionability of an exculpatory clause, but reversing summary judgment as to allegations of misrepresentation by defendant of alarm system's features and capabilities.)

A. Development of Software Products Liability

A journey through the history of case law involving alleged tort liability in computer software can begin with *Jaskey Finance and Leasing and Samrus Corp. v. Display Data Corp.*⁴⁶ In *Jaskey*, plaintiff purchased a computer system and installation and maintenance services for the system. The computer system failed to operate properly, resulting in damages and further economic loss of obtaining alternate computer time.⁴⁷ Plaintiff alleged that the computer equipment and programs were negligently designed and insufficient to perform their contemplated tasks.⁴⁸ The court, in dismissing the case, held that plaintiff's damages only amounted to the loss of value of the computer system and the accompanying replacement costs, and characterized the claim as one sounding in contract, not tort.⁴⁹ Subsequent cases in various jurisdictions echoed this holding, applying the economic loss doctrine to cases involving loss to the product.⁵⁰

The fears arising from the so-called Year 2000 (Y2K) “bug” mobilized numerous parties to litigation.⁵¹ As it turned out, the Y2K problem had more bark than bite; ironically, much of the Y2K litigation stemmed from software problems that arose *before* the new millennium. The Y2K

⁴⁶ 564 F. Supp. 160 (E.D. Pa. 1983).

⁴⁷ *Id.* at 162.

⁴⁸ *Id.* at 166.

⁴⁹ *Id.*

⁵⁰ *See, e.g.,* *Affiliates for Evaluation v. Viasyn Corp.*, 500 So. 2d 688 (Fla. App. 1987), where, in a case similar to *Jaskey*, *supra* note 46, the court held that the damages in dispute were purely economic and thus sounded in contract and not in tort.

⁵¹ *See generally*, SUZANNE R. ESCHRICH, *THE YEAR 2000 – DELIGHT OR DISASTER: VENDOR LIABILITY AND THE YEAR 2000 BUG IN COMPUTER SOFTWARE*, 4 B.U. J. SCI. & TECH. L. 8 (1997).

problem, which was the inability of many computer systems and software to recognize four-digit year integers, began to cause problems for computer users in the 1990s as the processing of future dates started triggering compatibility errors in the users' systems. A common example was credit card processing software being unable to acknowledge the entry of a 21st century card expiration date.⁵² This resulted in much class-action litigation, as numerous small software customers banded together to take action against software vendors that were aware of the impending Y2K problem but reluctant to provide necessary upgrades for free or reasonable cost.⁵³ Many of these actions were based on theories of scienter and fraud, as the vendors were allegedly "cashing in" on Y2K fears by charging for upgrades.⁵⁴ Ultimately, many such cases settled, often with the vendor agreeing to provide Y2K upgrades for free.⁵⁵ The standard for liability in Y2K litigation is similar to other liability cases involving economic damage, requiring an intentional tort by the defendant, such as fraud or misrepresentation.⁵⁶

Some plaintiffs have attempted to obtain remedies for damages caused by software problems on a theory of professional malpractice, usually directed at computer programmers or

⁵² See, e.g., *Produce Palace, Int'l v. All Am. Cash Register, Inc.*, No. 97-CV-03330 (Mich. Cir. Ct. filed June 12, 1997).

⁵³ See REED R. KATHREIN, *CLASS ACTIONS IN YEAR 2000 DEFECTIVE SOFTWARE AND HARDWARE LITIGATION*, 18 REV. LITIG. 487 (1999).

⁵⁴ *Id.* at 500.

⁵⁵ *Id.* at 499-502.

⁵⁶ See *Peerless Wall and Window Coverings, Inc. v. Synchronics, Inc.*, 85 F. Supp. 2d 519 (W.D. Penn. 2000) In a class action against manufacturer of non-Y2K compliant mass-marketed software, plaintiff alleged breach of contract, express and implied warranties, fraud and negligent misrepresentation. The court granted summary judgment for defendant, stating that the warranty claims were disclaimed by the user agreement, and that the fraud and misrepresentation claims were not actionable, due to a lack of reliance. The court further stated that the economic loss doctrine requires parties in privity to "look to the contract itself for their remedies."

consultants. However most courts do not view such defendants as “professionals” in the context of malpractice liability.⁵⁷ The uncertain level of legal duty given to computer employees is due in part to a lack of technical and manufacturing standards in the industry.

The question as to whether software constitutes a “product” in terms of products liability remains unresolved. Is computer software a tangible good, or merely informational content? In examining at the “information” side of the question, it should first be noted that only a few very specific types of informational content have been subject to liability for defects. Navigational charts are perhaps the clearest example of this.⁵⁸ By contrast, liability in tort was not found in cases involving allegedly defective publications such as encyclopedias⁵⁹, how-to books⁶⁰, and medical textbooks.⁶¹ One can make a distinction between the two groups of informational content and discern the reasoning behind the disparate treatment in the courts. Pilots *must* rely on

⁵⁷ See *Analysts International Corp. v. Recycled Paper Products, Inc.*, No. 85 C 8637, (N.D. Ill. 1988), holding that, in Illinois, actions for professional malpractice are barred. The court in *Analysts* did allow to stand plaintiff’s claim for false and misleading advertising. See also *Hospital Computer Systems v. Staten Island Hospital*, 788 F. Supp. 1351 (D. N.J. 1992), holding that computer consultants do not meet the standard of “professionals,” and that such consultants can be held liable only for ordinary negligence. *But see Diversified Graphics v. Groves*, 868 F.2d 293 (8th Cir. 1989), holding computer consultants to an elevated standard of care, due to their superior knowledge and expertise in computer systems.

⁵⁸ See *e.g.*, *Aetna Cas. & Sur. Co. v. Jeppesen & Co.*, 642 F.2d 339 (9th Cir. 1981). The courts in cases involving liability for defects in navigational charts have noted the reliance placed by pilots on such charts.

⁵⁹ In *Winter v. G.P. Putnam’s Sons*, 938 F.2d 1033 (9th Cir. 1991), plaintiffs had relied on information in defendant’s book, *The Encyclopedia of Mushrooms*, to distinguish safe from unsafe mushrooms. Plaintiffs picked and ate what they believed were safe mushrooms, however the mushrooms ingested were in fact poisonous, resulting in serious medical problems for plaintiffs, including liver transplants. Nonetheless, the Ninth Circuit affirmed the trial court’s grant of summary judgment for the defendant. The court reasoned that the publisher had no duty to investigate the accuracy of the contents of its publication, and that information in the publication constituted ideas, rather than a product.

⁶⁰ *Alm v. Van Nostrand Reinhold*, 480 N.E.2d 1263 (Ill. 1985). (Plaintiff injured while making tool listed in book, *The Making of Tools*).

⁶¹ *Jones v. J.B. Lippincott Co.*, 694 F. Supp. 1216 (D. Md. 1988). (Nursing student injured treating self with constipation remedy listed in nursing textbook).

navigational charts - the safety of air travel hinges on the accuracy of such charts - therefore the charts are viewed as a safety tool developed for the pilots' use. By contrast, media such as encyclopedias, textbooks, how-to manuals and the like are usually intended as informative, entertainment or tutorial devices, intended for more general audiences, and as such are not considered "products" by the courts, as holding such material to products liability standards would create a chilling effect upon authors and publishers.⁶²

The Ninth Circuit suggested in dictum that computer software might be considered a product for purposes of strict products liability in tort,⁶³ though there are no cases on point to legitimize this view.⁶⁴ Nonetheless, this opinion could be viewed as a signpost for future interpretation by the courts that software is a product. Further strengthening the software-as-a-product argument is the fact that computer programs are generally considered patentable subject matter.⁶⁵ Patentability requires that the subject matter have functionality;⁶⁶ mere expressions or algorithms are not sufficient for obtaining patent protection. Finally, the Restatement⁶⁷ expresses the distinction that computer software that is mass-marketed is considered a good,⁶⁸ while

⁶² Alm, *supra* note 60, at 1267. "Plaintiff's theory, if adopted, would place upon publishers the duty of scrutinizing and even testing all procedures contained in any of their publications."

⁶³ RESTATEMENT, *supra* note 12, § 19 cmt. d. at 278 (citing *Winter v. G.P. Putnam's Sons*, *supra* note 59)).

⁶⁴ *Id.*

⁶⁵ *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994)(en banc).

⁶⁶ 35 U.S.C. § 101 sets forth the requirement that the subject matter be "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" to obtain a patent.

⁶⁷ RESTATEMENT, *supra* note 12, § 19 cmt. d. at 278-9.

⁶⁸ *See e.g.*, *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670 (3d Cir. 1991).

computer software that is developed specifically for the customer is considered a service.⁶⁹

Firewall software manufactured developed for use by individuals and small organizations would likely fall into the first category, as it is generally purchased as an “off-the-shelf” item.⁷⁰ However the lines between product and service may be blurred when dealing with security software used by commercial users. Is the software of a standard form that is simply adapted to the end user’s needs, or is the program designed specifically per user specifications as a custom “turn-key” application? The latter instance would likely constitute a service; the former could arguably be labeled a product. The distinction could turn on whether the manufacturer has sold a substantially similar product to other customers, in which case the software may be considered a product. Even so-called “custom” software installations are sometimes built upon a common generic design and later tailored to the specific application, arguably thrusting such programs into the “mass-produced” category. The goods/services distinction of custom software is further muddled by the disparate treatment of the question by courts in different jurisdictions.⁷¹

The Uniform Computer Information Transactions Act (UCITA) was created as an attempt to remedy the shortcomings of the UCC’s ability to effectively address the intangible nature of electronic information systems. Originally proposed as Article 2B of the Uniform Commercial

⁶⁹ See *e.g.*, *Micro-Managers, Inc. v. Gregory*, 434 N.W.2d 97 (Wis. Ct. App. 1988).

⁷⁰ An example of such an off-the-shelf firewall program is Zone Alarm, a firewall program designed for use by owners of personal computers who utilize Internet connections. <<http://www.zonelabs.com>>

⁷¹ In *Micro Data Base Systems, Inc. v. Dharma Systems, Inc.*, 148 F.3d 649, 654 (1998), the Seventh Circuit criticized this disparity when it pointed out that the lone Indiana case, *Data Processing Services, Inc. v. L.H. Smith Oil Corp.*, 492 N.E.2d 314 (1986), held that custom software is a service, while the sole New Hampshire case, *Colonial Life Ins. Co. v. Electronic Data Systems Corp.*, 817 F. Supp 235 (D. N.H. 1993), held that it is a good. The court in *Micro Data Base Systems* sided with the New Hampshire decision in holding that custom software is a good, and subject as such to the U.C.C.

Code, UCITA did not arise without controversy⁷². Indeed, the American Legal Institute (ALI) withdrew its support of UCITA due to the Act's pro-industry stance.⁷³ Some critics believe that UCITA weakens consumer rights by the Act's confusion of warranty law.⁷⁴ UCITA's distinction between informational content and published informational content is troublesome to some commentators.⁷⁵ Common examples of published informational content include multimedia encyclopedias and online databases, which have historically been protected in print media from tort liability. UCITA exempts from liability published informational content; no implied warranties arise. However this exemption is potentially over broad, as the exclusion could include such items as user manuals, or even components of computer programs, such as user interfaces.⁷⁶ Such an exemption may be used as a shield to avoid liability for defects.⁷⁷ Proponents of UCITA contend that the statute was not intended to be consumer protection legislation; rather, a commercial code modeled after the UCC.⁷⁸ Supporters also believe that supplementing UCITA with provisions giving broader rights and warranties to consumers will force vendors to increase prices and force out smaller software developers.⁷⁹ At the time of this writing, UCITA has been

⁷² AJAY AYYAPPAN, UCITA: UNIFORMITY AT THE PRICE OF FAIRNESS?, 69 Fordham L. Rev. 2471, 2472 (2001).

⁷³ *Id.* at 2473.

⁷⁴ *Id.* at 2508.

⁷⁵ *Id.* at 2509.

⁷⁶ *Id.*

⁷⁷ *Id.* at 2510.

⁷⁸ *Id.*

⁷⁹ *Id.* at 2511.

adopted by two states, Maryland and Virginia.⁸⁰ It should be noted, however, that the adoption of UCITA has been vigorously opposed by the Attorneys General of 26 states⁸¹ and sharply criticized by the Federal Trade Commission.⁸²

B. Burglar and Fire Alarms: Analogous Case Law That May Have a Bearing on Software Liability

In examining potential tort liability for damages caused by defective security software, a parallel can be drawn with cases involving damages caused by defective burglar alarm systems. There is much case law concerning alarm systems, with varied outcomes. It is worth analyzing this area of case law as it might be possible to apply some of its elements to security software tort cases.

There are certain circumstances under which a tort claim may be actionable for defects in a burglar alarm system. However, to sustain such actions, courts have generally required a higher level of wrongful conduct by a defendant, such as gross negligence or misrepresentation.⁸³ As with products in general, absolute effectiveness of alarm systems is not a guarantee. Burglar

⁸⁰ UCITA Online, <<http://www.ucitaonline.com/whathap.html>>

⁸¹ Statistics compiled by Cem Kaner, last modified July 22, 1999, <<http://www.badsoftware.com/oppose.htm>>

⁸² <<http://www.ftc.gov/be/v990010.htm>>

⁸³ See Mankap, *infra* note 45. See also *Douglas W. Randall, Inc. v. AFA Protective Systems, Inc.*, 516 F. Supp. 1122 (E.D. Pa. 1981) (Upholding jury award to plaintiff after defendant's employee turned down the sensitivity level of alarm system, causing system to fail to detect entry of an intruder. The contract clause limiting defendant's liability to \$250 for negligence held inapplicable in the instant case of gross negligence.)

alarm companies will often place caveats in warranty language expressing that their products will not prevent burglaries.⁸⁴ Such language is often fairly bargained for by the parties and will usually be held as valid in cases involving ordinary negligence.⁸⁵ However, there is at least one case in which a limitation of damages clause for a burglar alarm system has been voided.⁸⁶

Cases involving alarm systems deactivated by burglars provide an interesting parallel to computer systems breached by hackers. Both types of cases involve an intervening criminal act occurring between the alleged conduct of the defendant and damage to the plaintiff. Both types of cases also involve breaches that are foreseeable by the contracting parties.

In cases involving personal injuries or deaths due to defective products, strict liability is invoked.⁸⁷ In personal injury cases where a defective fire alarm is the cause, the case law likewise favors applying strict liability.⁸⁸ Furthermore, personal injury cases where liability is not found tend to be due to factors outside the realm of strict liability concepts.⁸⁹

⁸⁴ Mankap, *infra* note 45.

⁸⁵ *Id.*

⁸⁶ DCR, Inc. v. Peak Alarm Co., 663 P.2d 433 (Utah 1983) (holding that a liquidated damage clause, while generally held as valid between informed parties expressing mutual intent, was in the instant case void, due to the failure of the language to “clearly and unequivocally” express intent).

⁸⁷ *See, generally*, KEETON, *supra* note 21, § 98.

⁸⁸ *See, e.g.*, Interstate Engineering, Inc. v. Burnette, 474 So. 2d 624 (Ala. 1985) (affirming plaintiff verdict in wrongful death action due to failure of heat detector to raise alarm during house fire); Butler v. Pittway Corp., 770 F.2d 7 (N.Y. 1985) (in reversing trial court’s summary judgment that favored defendant on ground that detectors had not caused fire, the higher court reasoned that the alarm’s failure to sound was nonetheless attributable to the plaintiff’s loss as proximate cause is not limited to situations in which a defect causes accidents).

⁸⁹ *See, e.g.*, Estate of Whittington v. Emdeko Nat. Housewares, Inc., 422 N.E.2d (Ill. App. 1981) (affirming judgment for defendant manufacturer in strict liability action because plaintiff could not recall having replaced the heat detector’s batteries in 4 years, nor could she recall if she even heard the alarm at all); Otis v. Scientific Atlanta, Inc., 612 S.W.2d 665 (Tex. Civ. App. Dallas 1981) (summary judgment in favor of defendant affirmed on the ground that plaintiff’s action was barred by limitations).

C. Fact Patterns That Conceivably Give Rise to Liability

Case law involving software tort liability has evolved very slowly. This is likely due to the fact that consequential damages caused by software defects are often economic in nature, and thus within the purview of contract remedies.⁹⁰ Because of the primarily economic nature of damages, courts are reluctant to hold software manufacturers to standards of liability beyond those set forth in contract law and allow those long-standing remedies to “drown in a sea of tort.”⁹¹ One commentator has even suggested that the computer information industry should be afforded the similar limitations of tort liability to those given the builders of waterways and railroads in the nineteenth century, arguing that “the builders of the National Information Infrastructure” should be free to allocate risk among themselves and users.⁹² Perhaps this view is derived from the idea that the information industry is still nascent and should be allowed some freedom to develop. But if this reasoning were to be held as true, it does not explain why manufacturers of computer *hardware* - parties who are also “builders of the National Information Infrastructure” - do not enjoy similarly protection from liability.⁹³ The hardware-software distinction appears to turn on

⁹⁰ See East River, *infra* note 40.

⁹¹ See *Id.*, at 874. Justice Blackmun expressed the court’s reluctance to extend tort liability into damages of a pure economic nature. “Products liability grew out of a public policy judgment that people need more protection from dangerous products than is afforded by the law of warranty ... it is clear, however, that if this development were allowed to progress too far, contract law would drown in a sea of torts.”

⁹² See RUSTAD, *infra* note 19, at 301.

⁹³ See *Shaw v. Toshiba America Information Systems, Inc.*, 91 F. Supp. 2d 926 (E. D. Tex. 1999). In *Shaw*, summary judgment was denied to defendant manufacturer of defective computer floppy disk controllers which allowed corrupted data to infect plaintiff’s data. Plaintiffs had brought suit under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(5), alleging that defendant, by means of its defective components, had caused the transmission of corrupted information, causing damage to plaintiff’s data. The court, in denying summary

the Restatement's continued view that computer software is intangible personal property, and thus not a product, per se.⁹⁴ In recent years, computer software has become the solution of choice in more and more systems, and is relied on to perform more complex tasks. Highly technical operations that only a few years ago were subject solely to human control are now becoming partially or completely automated due to the development of sophisticated computer programs.⁹⁵ In addition, the complexity of mass-marketed software is also increasing, enabling more applications to no longer require custom, service-type software solutions. As the application of software programs becomes more widespread and complex, it follows that the nature of damages arising from software defects will become more diverse. The time may come in the not-too-distant future when certain conduct by software manufacturers will fall squarely within the sights of tort liability.

Harms to persons or property can include economic loss, if the loss is caused by harm to: (a) the plaintiff's person; (b) another person when that harm interferes with an interest of the plaintiff protected by tort law; or (c) the plaintiff's property other than the defective product itself.⁹⁶ Economic loss resulting from harm to the plaintiff's person commonly includes loss or reductions of earnings.⁹⁷ Establishing a claim for losses to plaintiff's property other than the

judgment, held that defendant had not only anticipated the defect in the controllers, it had actually known about it.

⁹⁴ RESTATEMENT, supra note 12, § 19.

⁹⁵ FRANK D. NGUYEN, REGULATION OF MEDICAL EXPERT SYSTEMS: A NECESSARY EVIL?, 34 Santa Clara L. Rev. 1187 (1994). A striking example of such a new technology is the development of "medical expert systems," where medical data stored in databases are utilized by interactive computer systems to assist doctors in the medical diagnostic process.

⁹⁶ RESTATEMENT, supra note 12, § 21.

⁹⁷ *Id.*, cmt. b.

defective product in software cases has been problematic, as the economic loss doctrine has been broadly interpreted by the courts.

The first case involving alleged liability for system data was *Transport Corp. Of America, Inc. V. IBM*.⁹⁸ In that case, the plaintiff sought damages under negligence and strict liability for damages it incurred when a failed disk drive in a computer system purchased from defendant destroyed plaintiff's data and rendered the system inoperable. The court in *Transport*, following Minnesota law and the doctrine in *East River Steamship*⁹⁹, not only denied recovery for the loss to the computer system itself, but also held that the plaintiff's lost data comprised part of an "integrated system" with the computer, thereby encompassing plaintiff's consequential loss of data within the economic loss doctrine.¹⁰⁰ In addition, because tort claims are only available for losses not contemplated by the contracting parties, the court found that plaintiff's remedies were limited to contract.¹⁰¹ Lost profits caused by defects are likewise held to be within the economic loss doctrine.¹⁰²

After decades of caselaw demonstrating the broad scope of the economic loss doctrine, and the contract remedies available in such actions, a successful negligence action for property damages arising from a software defect seems unlikely at this time. Indeed, some commentators on the subject of software products liability have expressed their doubts as to the likelihood of

⁹⁸ 30 F.3d 953 (8th Cir. 1994).

⁹⁹ See supra note 40.

¹⁰⁰ See *Transport*, supra note 98, at 956-57.

¹⁰¹ *Id.*, at 958.

¹⁰² See Moorman, supra note 41, at 82.

success for such actions.¹⁰³

1. Liability Arising From Personal Physical Injury

Applying tort law in software products liability cases involving physical harm certainly appear more feasible than applying tort law in claims for economic losses.¹⁰⁴ Such an application of tort law could find support in public policy. The costs of damages due to dangerous products are best absorbed by the merchandisers of said products. Such is viewed as a “risk-bearing economic” theory, rather than one of “deep pockets.”¹⁰⁵ Nearly forty years ago, strict products liability began its ascension into American jurisprudence with the holding that “[t]he remedies of injured consumers ought not to be made to depend upon the intricacies of the law of sales.”¹⁰⁶

Although there are no cases on point involving strict liability for software defects,¹⁰⁷ there have been a few cases where products liability claims have been raised or realistically could be raised under similar facts in the future.¹⁰⁸ In one particularly notable case, *Sparacino v. Andover*

¹⁰³ See, e.g., THOMAS G. WOLPERT, PRODUCT LIABILITY AND SOFTWARE IMPLICATED IN PERSONAL INJURY, 60 Def. Couns. J. 519, 522 (stating the difficulty in pinpointing an omission or commission by a defendant software manufacturer in an action for negligence). See also RUSTAD, supra note 19, at 246-47 (citing, among other problems, a lack of a defined standard of care for Internet security professionals).

¹⁰⁴ KEETON, supra note 21, § 98.

¹⁰⁵ *Id.*

¹⁰⁶ *Greenman v. Yuba Power Products, Inc.*, 377 P.2d 897 (Cal. 1963).

¹⁰⁷ See RESTATEMENT, supra note 63.

¹⁰⁸ See WOLPERT, supra note 103, at 519.

Controls Corp.,¹⁰⁹ a high school teacher suffered extensive injuries after inadvertently breathing poisonous chlorine gas during a chemistry experiment he was preparing early one morning at the school. The defendant company's microprocessor-based building control system, which was in use by the school, was programmed to allow activation of the chemistry lab's exhaust fans beginning at 6:30 in the morning. Since the plaintiff's chemistry experiment was conducted at approximately 6:00 A.M., the exhaust fans in the lab were not enabled for operation at that time, resulting in the plaintiff's exposure to the toxic gas. Naming manufacturer Andover and installer Communication Management Corp. (CMC) as defendants, plaintiff claimed, inter alia, that the control system was "inherently dangerous, defective and unreasonably unsafe in design and manufacture," claiming the system had no override capabilities and lacked sufficient warnings.¹¹⁰ The court, in affirming summary judgment in favor of the defendants, held that since the control system was designed and programmed to allow activation of the exhaust fans at normal school hours, there was no defect in the computerized system used by the school. It was held as not foreseeable that someone would be conducting a laboratory experiment during non-occupancy hours of the school. Andover had no duty to warn of the "merely conceivable danger that someone would be injured during a chemistry experiment performed during non-occupancy hours."¹¹¹ The facts given in the case make it debatable as to whether the design of the software programming of the control system falls within the responsibility of the manufacturer Andover, or installer CMC, or both. It is not known from the facts as to what obligations were created in the

¹⁰⁹ 592 N.E.2d 431 (Ill. App. 1992).

¹¹⁰ *Id.* at 433.

¹¹¹ *Id.*, at 436.

relationship between Andover and CMC. However, the facts of the case show that Andover had given “user instructions” to CMC for the purpose of programming the system for the school, and had even provided an instructional videotape to CMC, demonstrating how a customer could program the system.¹¹²

If one were to hypothesize a case with similar facts as *Sparacino*, but with injuries to a plaintiff being of a type reasonably foreseeable, liability could be found. An example might be a chemistry experiment being conducted during normal school hours, where a defect in the control system’s programming results in failure of the lab’s exhaust fan to safely remove toxic fumes and injuries are inflicted. If the responsibility of programming the operation of the system lies with the installer, that installer could be found liable in tort. Similarly, if the manufacture of the system were such that a software defect caused the fan’s operation to fail, liability could attach to the manufacturer. What is important in *Sparacino* is that the court’s decision in favor of the defendants turned on the lack of foreseeability, and did not rule out the possibility of liability arising from a true software or programming defect resulting in physical injury. Like the aforementioned hypothetical, one could quite easily envision many other fact patterns involving software defects that would subject persons to harms of greater foreseeability, rising well above the “merely conceivable danger” standard of *Sparacino*. In such scenarios, it would follow that ensuing tort actions could survive summary judgment and proceed to damage awards.

2. Liability Arising From Invasion of Privacy

¹¹² *Id.*

Decades before the development of computers and computer databases, Justice Brandeis issued an eerily prophetic opinion: “Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.”¹¹³ Today, government intrusion into personal affairs is not our only fear. With the growing number of organizations collecting and compiling detailed personal data, the temptation of theft of this data by computer hackers has become a major concern of many computer users.¹¹⁴

Invasion of privacy is a collection of torts generally divided into four categories: (1) appropriation of a person’s name or likeness;¹¹⁵ (2) false light in the public eye;¹¹⁶ (3) public disclosure of private facts,¹¹⁷ and (4) unreasonable intrusion.¹¹⁸ For the purposes of this discussion, the third and fourth categories will be examined as the types of actions most likely to arise from security breaches into computer systems.

To prevail on a claim for public disclosure of private facts, there are four requirements that must be satisfied: (1) the disclosure must be public; (2) the facts disclosed must be private; (3) the matter made public must be highly offensive and objectionable to a reasonable person; and

¹¹³ *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

¹¹⁴ *See, e.g.*, *supra* note 1.

¹¹⁵ *See* KEETON, *supra* note 21, § 117.

¹¹⁶ *Id.*, at 863.

¹¹⁷ *Id.*, at 856.

¹¹⁸ *Id.*, at 854.

(4) the public must not have a legitimate interest in having the information made available.¹¹⁹

Unreasonable intrusion is a separate tort that focuses on the manner in which private information has been obtained. For a claim to be actionable, a plaintiff must show that another has intentionally intruded, physical or otherwise, upon the plaintiff's seclusion or solitude, and that such intrusion would be considered offensive by a reasonable person.¹²⁰

There exist cases with fact patterns that have given rise to both public disclosure of private facts and unreasonable intrusion.¹²¹ Although both torts bear similarities, the two are separate interests that may be invaded, and many courts have allowed both to be actionable in the same case, as a claim of one tort does not necessarily preempt a claim for the other.¹²²

Databases compiled and maintained by organizations today contain nearly every conceivable type of personal information. Some personal information is particularly sensitive, such as a medical facility's records containing the identities of abortion patients, drug-treatment patients, or persons with HIV/AIDS. It has long been held that the state may compile databases of certain drug prescription information.¹²³ Due to the sensitive nature of certain data, the attractiveness of breaking into databases containing it would be irresistible to some computer

¹¹⁹ *Id.* at 856-57.

¹²⁰ *See, e.g., Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060, 1065 (Colo. App. 1998) (citing RESTATEMENT SECOND, TORTS § 625B (1981)).

¹²¹ *Id.*

¹²² *Id.* at 1065, citing *Wolf v. Regardie*, 553 A.2d 1213 (D.C. Ct. App. 1989) and *Robert C. Ozer, P.C. v. Borquez*, 940 P.2d 371 (Colo. 1997).

¹²³ *Whalen v. Roe*, 429 U.S. 589 (1977) (holding as constitutional the right of government to record computer files containing the identities and other information of all persons who have received doctors' prescriptions for drugs that also have illegal purposes).

malfeasants. The political or economic value of such data is enormous - a malevolent individual with an agenda could be motivated to obtain and disseminate sensitive personal data. It is not difficult to envision, for example, an anti-abortion activist hacking into the records of a family planning clinic, or a would-be blackmailer gaining access to potentially embarrassing medical information of individuals. Could a court assign liability to a manufacturer if a flaw in its security software program facilitates hacker access to sensitive personal data that results in an intrusion of a person's privacy? If one were to view the damage of intrusion in the same light as the damage of personal injury, such liability would be feasible.

It has been held that an Internet service provider (ISP) assumes a greater duty of care and is thus liable for damages resulting from the content conveyed onto the ISP's network by a user of the network, if the ISP has exercised some form of editorial control over the content submitted. In *Stratton Oakmont v. Prodigy Servs. Co.*,¹²⁴ online provider Prodigy was found liable for defamatory content placed on its bulletin board service.¹²⁵ Since Prodigy's service included a function for screening incoming content, the court viewed Prodigy as possessing editorial control, thus raising Prodigy's duty of care to that of a publisher.¹²⁶ The *Stratton* case was later superseded by statute, the Communications Decency Act of 1996 (the "Act"),¹²⁷ which protects

¹²⁴ 1995 WL 323710 (S.D.N.Y., May 26, 1995) (unpublished decision). Prodigy Services Co. provided an online bulletin board with means of screening objectionable language. Defamatory comments against Stratton Oakmont were posted on the bulletin board by an online user. Despite Prodigy's defense that it was merely a passive conduit of information, the court found Prodigy liable, arguing that Prodigy be held to the higher standard of a publisher, that Prodigy "is clearly making decisions as to content ... and such decisions constitute editorial control." *Id.*

¹²⁵ *Id.*

¹²⁶ *Id.*

¹²⁷ 47 U.S.C. § 230 (1996).

“interactive computer services” from publisher-level liability.¹²⁸ Since the Act’s language appears to be targeted primarily to online service providers,¹²⁹ the attachment of third-party liability framed in *Stratton* appears to remain intact. Indeed, the Congressional intent of the Act was to prevent a chilling effect upon Internet speech, to “maintain the robust nature of Internet communication,” and “to preserve ... the competitive free market that presently exists for the Internet and other interactive computer services.”¹³⁰ Although the liability of an ISP has been preempted by the Act, the gravity of court’s reasoning in *Stratton* must still be considered. The primary factor behind the court’s decision in *Stratton* was that Prodigy had provided a screening function to its bulletin board - a security feature. That this security feature was in place, and that it failed to filter the tortious language of the offensive user, is the focal point of the court’s elevation of Prodigy’s duty of care. While ISPs are now statutorily protected, we might apply this reasoning to a security software program: the intention of the software is to prevent unauthorized access to a computer system. If the software fails to stop an unauthorized entry into the computer system, and the unauthorized entry causes harm in the form of invasion to privacy, one might find liability for that harm.

¹²⁸ *Id.*, para. (c)(1) (stating that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

¹²⁹ *Id.*, para. (e)(2) (defining “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.”).

¹³⁰ *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (citing 47 U.S.C. § 230).

V. CONCLUSION

Finding tort liability for property damage due to a software defect seems reasonably unlikely, due to the broad scope of the economic loss doctrine and the growing tendency of the judiciary to apply contract remedies in such cases.¹³¹ Although there appears to be a growing public sentiment against software vendors,¹³² it remains to be seen if this sentiment filters its way into the caselaw. Despite its many critics, the further adoption of UCITA may actually provide a strengthening of manufacturers' immunity from tort liability.¹³³

While the present caselaw does not reflect a major judicial trend toward applying products liability theories against software manufacturers, there appear to be a few plausible fact patterns that would allow a finding of liability. A case involving personal injury due to a software defect could place a defendant manufacturer within the bounds of strict liability.¹³⁴ Any warranty language attempting to disclaim such liability might well be void as a matter of public policy.¹³⁵ Similarly, an invasion of privacy could be viewed in the same context: disclosure of personal facts

¹³¹ See supra notes 37 - 45.

¹³² One of the more striking examples of public contempt toward a software vendor is derived from the antitrust litigation against Microsoft Corp. For example, of the 47 public comments released on Feb. 15, 2002, by the U.S. Justice Dept., forty-two urged that Microsoft not be allowed to settle the case. Dan Richman, *Public Sentiment Runs Against Microsoft*, Seattle Post-Intelligencer, Feb. 16, 2002, at http://seattlepi.nwsourc.com/business/58557_microsoft16.shtml

¹³³ See supra notes 72 - 82.

¹³⁴ See supra notes 107 - 112.

¹³⁵ See supra note 37.

or intrusion could be seen as an injury requiring redress.¹³⁶

As some commentators have suggested, there may indeed be a protective wall surrounding software manufacturers that is unavailable to merchants of more traditional products.¹³⁷

However, this should not lead to a complacency on the part of software developers and manufacturers. All that is required is one case involving the right ingredients for a judge to decide to deny summary judgment - a case that, sooner or later, will occur.

¹³⁶ *See supra* notes 115 - 122.

¹³⁷ *See supra* note 92.