

Two Views on Security Software Liability

Let the Legal System Decide

Computers pervade the modern world and enable the creation, storage, processing, and communication of valuable property in the form of information assets. Computerized control systems manage banks, factories, retail inventories, air traffic control, hospitals, schools, corporations, and government organizations. Computers

consumers to rely on the expertise of those who provide such products to ensure their reliability. Thus, warrant of fitness for a particular purpose provides an attractive basis for assessing strict liability.²

Assessing liability for the design, manufacture, or sale of defective products—and for failure to warn consumers of the dangers inherent in products—is a well-established function of tort law. Security software products would seem to be perfect examples of applicability of tort liability because organizations and individuals rely on such products to protect themselves and their property.

However, because tort liability treats personal injuries, property injuries, and purely economic injuries differently, software product manufacturers are escaping liability for some damage caused by their defective products by using contractual clauses in purchase contracts and licenses that disclaim liability. Because of security software products' importance in protecting IT infrastructures of individuals, organizations, and the nation, making sure that liability is

DANIEL J. RYAN
Law Offices of Daniel J. Ryan

and their software programs are embedded in our cars, boats, trains and planes, in tools, equipment, and machinery, in telecommunications systems and public switched networks, even in our bodies. Consequently, software products play an integral role in every aspect of our lives, and, when they are not reliable, pose a danger to people, to tangible and intangible property, and to our economic security as individuals and as a nation.

Some software products are designed specifically to enhance security. Such products are supposed to protect our property and us, to detect intrusions by outsiders or abuses of privilege by insiders, and to facilitate rapid and effective response that minimizes damage and promotes rapid recovery to operational readiness. These include access control systems, anti-malicious code detection and eradication programs, intrusion detection systems, backup systems and beta sites, and a host of other security applications and utilities.

The failures of such programs and systems represent especially grave dangers because, in part, of the trust

we place in them to ensure our security and the security of the nation's critical infrastructures. Despite these concerns, or perhaps because of them, manufacturers and sellers insist that sales orders and licenses contain disclaimer clauses that absolve them from liability for defects.¹

Product liability is a necessity

As a practical matter, consumers cannot create their own security software to avoid having to purchase commercial products. They're also not in the best position to thoroughly test security software products. It is entirely reasonable for con-

Do software defects belong in court?

70 Let the Legal System Decide, by Daniel J. Ryan

73 Using the Right Legal Tools, by Carey Heckman

assessed for security software product defects is essential.

Tort liability for injuries caused by defective products satisfies several goals of modern society. Victims and their families should be compensated for injuries caused by defective products. Risk should be shifted from the consumer to the designer, manufacturer, or seller if the dangerousness of a product is not reflected in the price, especially where the risk-distribution benefits of the shift outweigh detriments. The manufacture, sale, and marketing of unsafe products should be deterred. Assessing liability when products cause injury also facilitates accountability. For these reasons, strict tort liability has evolved as a consumer remedy for personal injury, replacing outmoded restrictions based on privity of contract, notice of breach, and other contractual limitations of liability.³

Public policy requires that responsibility be assessed wherever it will most effectively reduce the risks inherent in defective products.⁴ Clearly, designers and manufacturers are better able than consumers to anticipate hazards and guard against their effects. Moreover, the damages that result from flawed security software can be overwhelming for an injured individual, while a manufacturer can insure against risk of injury or can adjust the price of the software so the risk is distributed among the public as a cost of doing business. The courts have stated that even if injuries are infrequent, “the risk of their occurrence is a constant risk and a general one. Against such a risk there should be general and constant protection and the manufacturer is best situated to afford such protection.”⁵

Unfortunately, courts have not applied tort liability concepts evenly, usually applying strict liability where a consumer suffers personal injury by a defective product. The cases are less clear when the damage is to property, and when the damages are purely economic, involving no physical

damage to persons or property,⁶ the courts often accept and enforce contractual disclaimers of liability by designers, manufacturers, and sellers of defective products in sales contracts or licenses.

Dueling with disclaimers

Because the courts recognize the validity of such restrictions,⁷ even in shrink-wrap or click-through contracts, manufacturers and sellers of software products have little incentive to work hard to ensure that their programs are bug-free. On the contrary, their incentive is to load their licenses with as many disclaimers as possible.

Such clauses are likely to be ineffective in actions for strict tort liability in which personal injury results from software product failure, such as might flow from collapse of the air traffic control system or failure of the 911 emergency response capabilities of the public switched networks. They are more likely to be effective where there is physical injury to property, and most likely to be enforced by the courts when physical damage to persons or property cannot be shown and damages are purely economic in nature.

Absent legislative tort reform to require that strict liability apply in all such cases, the courts must build on time-tested theories of warranty of fitness, misrepresentation, abnormal danger, negligence, fraud, lack of clarity, and unconscionability to find liability for all security product failures.

The doctrine of unconscionability has been widely applied where the parties to a contract with disclaimers are significantly unequal in bargaining power, as is certainly the case with security software products. Where safety is not an issue, courts are more likely to recognize disclaimers.⁸ Where safety is an issue, courts have invalidated disclaimers.⁹ Safety is, of course, the *raison d'être* of security software products.

Security software designers,

What's on the horizon?

Here you'll find lively discussions (and occasionally a knock-down, drag-out fight) about some of the major trends that we expect will impact security and privacy technology in the not-too-distant future. We do this with some risk, as anyone would who consulted a crystal ball to peer into the future of security and privacy. But we are undaunted. Our mission is to try to recognize and understand where things are heading and to think about their impact on security and privacy issues. We ask you to read these musings carefully, with your thinking cap firmly in place. We expect and welcome your feedback.

On our maiden voyage, we explore a controversial topic using a point/counterpoint format: Should software vendors be liable for defects in their products that result in security exposures for the users?

With Microsoft's touted Trustworthy Computing Initiative, spurred by the Gates memo of January 2002 (www.computerbytesman.com/security/billsmemo.htm) and the advent of business-related groups such as the Sustainable Computing Consortium (www.sustainablecomputing.org) now is an excellent time for security practitioners to explore the role of liability in making software more secure. Consider this: are these initiatives a way for software vendors to escape the threat of government regulation? Are armies of lawyers the ultimate threat? Another question to ponder while reading the Gates memo is what effect the software liability threat might have had on the business aspects of this critical strategic sea change.

Controversy is sometimes a good indicator of future technology trends that require more thinking through. As part of our job as prognosticating editors, we plan to seek out controversial issues and dig into them from a technical perspective. We might not always end up with clear answers, but we're certainly willing to foster the debate.

In the future months, we plan to unveil

continued on p. 72

manufacturers, and sellers argue that software products are complex and that it is impossible, or at least impractical, and prohibitively expensive to eliminate all bugs. They assert that assessing liability for negligence in a software products context would expose manufacturers and sellers to “damages of unknown and unlimited scope.”¹⁰ But recovery in product liability, whether in tort or warranty, is usually limited to foreseeable damages, so this argument is unconvincing.

continued from p. 71
such topics as:

- TCPA and Palladium (security processing Nirvana or Big Brother’s box)
- Web Services and security (cutting through the hype)
- Wireless security (especially 802.1X)
- Geographic computation (personalization boon or the ultimate in invasion of privacy?)
- Subscription services and security (how can we safely rent computation?)
- Software security analysis (getting past the buffer-overflow obsession)
- Embedded Internet systems (you connected *what* to the Net?)
- Ubiquitous computing (what happens when CPU cycles are everywhere)
- Peer-to-peer security (why Napster was seen as the big bad wolf)

We sincerely hope that you will suggest interesting topics and authors. Tell us what you want to see. Cross things off our list. Put other things on. We will avoid stilted academic-speak at all costs, seeking to foster realistic debate in an informal and lively style. And just to keep you on your toes, we’ll draw from a kaleidoscope of styles, with formats ranging from essays and interviews, to point/counterpoint debates. We look forward to hearing from you.

—Nancy Mead and Gary McGraw

Mead and McGraw are Security & Privacy task force members. For more on them, see page 8.

Most egregious are licenses that disclaim liability for defects that are known to exist at the time of manufacture or sale, such as buffer overflows, for example.

Safety is the *sine qua non* of security software products. The importance of using such products to protect the critical infrastructures upon which our organizations, our nation, and we depend for economic security, means legislation to extend strict liability for all defects in security software is desirable. Absent such legislation, courts can find disclaimers of liability for product failures to be unconscionable on the basis of the inequality in bargaining power between providers of security software products and consumers who have no choice to rely on them. The courts can combine policies of safety promotion and unconscionability to provide a convincing rationale for invalidating disclaimers of liability, and which rationally allocate responsibility to manufacturers and distributors, who are better able than consumers to ensure the reliability and safety of security software products.

References

1. http://www.businessweek.com/magazine/content/02_11/b3774071.htm.
2. UCC § 2-315 provides a warranty of fitness for a particular purpose. The fitness warranty is one of strict liability, although negligence is often present as well. One court stated, “... between strict liability under § 402A and warranty liability, the warranty predicate, fitness for ordinary purposes, appears to set a lower liability threshold that is more beneficial to the plaintiff. It also appears easier for the jury to understand and apply.” *Zacher v. Budd Co.*, 396 N.W.2d 122, 140; 1986 S.D. LEXIS 338; CCH Prod. Liab. Rep. P11,188 (S. D. 1986)
3. Comment m, Restatement of Torts (Second) § 402A.
4. *Escola v. Coca Cola Bottling Co. of*

Fresno, 24 Cal. 2d 453, 462; 150 P.2d 436, 440; 1944 Cal. LEXIS 248, (Cal. 1944)

5. *Escola* at 462.
6. The Restatement of Torts (Third), which has found less than universal acceptance among the States, takes the position that personal injury may not be disclaimed, but leaves open the question of the effectiveness of disclaimers for physical damage to property of for purely economic loss. § 18.
7. Of course, the courts do not recognize contractual limitations that are unconscionable, oppressive or unfair.
8. See, for example, *Petry v. Cosmopolitan Spa Intern.*, 641 S.W.2d 202; 1982 Tenn. App. LEXIS 421 (Tenn. App. 1982)
9. Consider the reasoning in *West v. Caterpillar Tractor*, 336 So. 2d 80; 1976 Fla. LEXIS 4448; 24 U.C.C. Rep. Serv. (Callaghan) 1154 (Fla. 1976); *Florida Steel Corp. v. Whiting Corp.*, 677 F. Supp. 1140; 1988 U.S. Dist. LEXIS 44; CCH Prod. Liab. Rep. P11,756 (M. D. Fla. 1988). While the issue was specifically personal injury, the reasoning could be applied more broadly to property and economic injuries, especially where other public policies support such application.
10. See *Seely v. White Motor Co.*, 63 Cal. 2d 9; 403 P.2d 145; 45 Cal. Rptr. 17; 1965 Cal. LEXIS 155; 2 U.C.C. Rep. Serv. (Callaghan) 915 (Cal. 1965)

Daniel J. Ryan is an attorney in private practice and an adjunct professor for The George Washington University in Washington, D.C., where he teaches cyberlaw and information security. He received a BSc degree in mathematics from Tulane University, an MSc in mathematics from the University of Maryland, an MBA from California State University, and a JD from the University of Maryland. He is a member of the Bar in Maryland and the District of Columbia, and a member of the ACM. He is a coauthor of *Defending Your Digital Assets* (McGraw-Hill Osborne Media, 2000), and has published numerous articles on law and technology. Contact him at danryan@danjryan.com or through his Web page at www.danjryan.com.