

**In Defense of Tort Law** by Thomas H. Koenig and Michael L. Rustad, (New York: New York University Press, 2201) ISBN: 0-8147-4757-6, pp. 320.

Book Review Essay by Thomas H. Koenig, Professor of Sociology & Law, Policy & Society, Northeastern University and Michael L. Rustad, Thomas F. Lambert Jr. Professor of Law & Director of High Technology Law Program Suffolk University Law School

Interviewer: Rob McNamara, Book Review Editor,  
Journal of High Technology Law  
Suffolk University Law School

### **What is your key purpose in writing this book?**

One of our goals was to cut through the rhetoric surrounding American tort law and present the best empirical research on how tort law actually operates. We believe that when people understand the functions of tort law and its role in creating a safer and more humane society, they will support an expansion of tort rights. Corporations have successfully waged a public relations campaign to create the false impression that most lawsuits are spurious, when in fact the opposite is true: tort law is a key guardian of American values. **In Defense of Tort Law** is the first book to provide a systematic study of the positive functions of tort law in contrast to tort reform literature produced by authors such as Peter Huber and Walter Olson. Peter Huber's **Liability**, for example, argues that liberal judges have completely undermined our civil litigation system. In contrast, we describe the strengths of the tort law system and its unique role in protecting women, minorities, and consumers. We use compelling case studies to illustrate the social role of tort law as well as reviewing statistical evidence to show the important societal role played by punitive damages litigation. The book dispels myths about the civil justice system so that tort law can continue to protect Americans in the new millennium.

We wrote **In Defense of Tort Law** to test the claim that tort law is in need of radical reform. Our book shows that most of the claims of the tort reformers are either seriously misleading or simply untrue. We use compelling case studies to show how tort remedies vindicate the rights of women, minorities, and ordinary Americans. The book is written in an accessible style so that law students, social scientists and interested laymen could understand the past, present and future of tort law. **In Defense of Tort Law** summarizes our decade long empirical study of patterns of litigation in U.S. tort law. Vice President Quayle's Council on Competitiveness claimed that punitive damages were responsible for destroying American productivity.<sup>1</sup> No database existed that could be used to test the tort reformers' assertion that punitive damages were skyrocketing out of control. We compiled the first nationwide database that examined patterns of awards. We found that punitive damages were rarely awarded, frequently reduced on appeal, and proportional to compensatory damages. We then examined punitive damages and non-economic damages (pain & suffering) in medical malpractice cases. Here, we found evidence that men and women employ tort remedies differently. . At every age group, women had a higher rate of non-pecuniary damages. Women were far more likely than men to be awarded non-economic damages for medical malpractice. Women were disproportionately injured by sexual abuse, nursing home malpractice, and, of course, loss of fertility. Our findings were that medical verdicts were even uncommon than in product liability cases. The real runaway verdicts are in business versus business tort cases and intellectual property litigation. The U.S. Supreme Court in *Honda Motor Co. v. Oberg*<sup>2</sup> referred to our study of punitive damages as the most comprehensive ever completed

---

1 Michael L. Rustad & Thomas Koenig, "The Historical Continuity of Punitive Damages Awards: Reforming the Tort Reformers," 42 Am. U. L. Rev. 1269, 1275-76 (1993).  
2 512 U.S. 415, 433 (1994).

## **What impact has your research had?**

Legal academics and practitioners have cited and built upon our work. We now have a solid body of empirical knowledge about American tort litigation that builds upon our work including excellent studies of law professors such as Marc Galanter, Lucinda Finley, Andrew Popper, Michael Saks, Neal Vidmar, Joseph Sanders, Ted Eisenberg and his collaborators at The National Center for State Courts. Every empirical study has confirmed our basic findings that punitive damages are rarely awarded, tightly controlled, and levied almost exclusively for truly egregious misconduct. We published our findings in a variety of top law reviews including the *Wisconsin Law Review*, *Michigan Journal of Law Reform*, *American University Law Review*, *Rutgers University Law Review*, *Iowa Law Review*, *North Carolina Law Review*, and *Products Liability Law Journal*. Professor Koenig and I testified in the U.S. Senate and U.S. House of Representatives. Our findings have been extensively reported in the *Wall Street Journal*, *The Economist*, *The New York Times*, *ABC News*, and hundreds of other media outlets. Perhaps the biggest impact has been in the courts. The Ohio Supreme Court and the Illinois Supreme Court struck down their omnibus tort reform statutes finding no empirical support for a torts crisis citing our research. We have written a large number of *amicus* briefs in state and federal courts throughout the country drawing upon our data.

## **Is this a publication for both practitioners and students?**

We provide extensive case law support for practitioners trying cases in diverse substantive fields including medical malpractice, products liability, premises liability, and Internet law. Our presentation of the policy arguments will be of interest to trial lawyers as well as the defense bar. Corporate counsel will appreciate our preventive law pointers on avoiding or limiting liability. The chapter on Internet law provides guideposts for limiting liability in online transactions. Legislators and other policymakers are given guidance on how to interpret statutory reform proposals. In the past, we could refer journalists to law review articles that were less accessible than this book. This book is written in a readable style and provides a single source book that explains how the tort law system works. Our table of cases includes most of the important cases covered in first year torts classes. We trace the development of torts over the last 200 years showing how each age in Anglo-American law reflects the social and historical context. For example, the torts of criminal conversation and seduction only make sense within the patriarchal context. Today's tort action to punish intentional infliction of emotional distress in a virtual reality or a listserv only became necessary with the rise of World Wide Web. Students tell us that they find the discussion of the path of tort law extremely valuable for comprehending the big picture. I am assigning this book as supplemental reading for my first year torts class. Professor Koenig is using the book in his theories of law and policy doctoral class at Northeastern University.

## **Is there a common theme in your book?**

Our thesis is that tort law has served as a public guardian from eighteenth-century England to the age of the Internet. Tort remedies evolve to meet the abuses of power in every age. In the eighteenth century, the remedy of exemplary damages was used to punish and deter abuses by the King and his agents as well as harms caused by arrogant aristocrats. In every era, tort remedies have evolved to protect Americans. In the eighteenth century, tort remedies punished and deterred powerful aristocrats who trampled on the rights of ordinary citizens. The first punitive damages award was handed down in 1763 in the famous English case of *Wilkes v. Wood*. In that case, the King's government conducted a warrantless search in an illegal and oppressive manner. Punitive damages teach even the most powerful defendant that "tort does not pay." In the nineteenth century, intentional torts expanded to counter misbehavior by the agents of railroads, utilities, and streetcar companies. The development of negligence or accident law emerged in the 1850s to counter abuses of corporate power such as building an unsafe bridge, railway bed, or unsafe workplace. Thousands were killed in railway accidents each year before tort law succeeded in deterring unsafe practices. In the second half of the twentieth century, tort law developed new causes of action

such as product liability, medical malpractice, premises liability, wrongful discharge, nursing home negligence, and psychiatric malpractice. The new tort of outrage recognized by Section 46 of the Restatement of Torts evolved to punish racists, sexual harassers, hate crimes, and extreme bullying in the workplace. Today, tort law is again evolving to punish and deter online defamation, the spread of computer viruses, online terrorism or stalking, e-mail spammers, identity thieves, the invasion of privacy, and fraudulent online marketing schemes. Our thesis is that strong tort law will become even more essential in the next century. The path of tort law has been to moderate and mediate abuses of power in every historical period. Without viable tort remedies, corporations suffer no significant penalty when they choose to endanger the consuming public in order to enhance profits.

Our argument is that private litigants serve the public interest by exposing dangers and risks that have gone unnoticed by regulators and the criminal side of the law. Second Circuit Judge Jerome Frank in *Associated Industries v. Ickes* first articulated the concept of the “private attorney general.”<sup>3</sup> Judge Frank used the term to refer to “any person, official or not, who brought a proceeding . . . even if the sole purpose is to vindicate the public interest . . . Such persons, so authorized, are, so to speak, private Attorneys General.”<sup>4</sup> Private attorneys general have played a critically important role in modern tort law as well as in their role of cooperating with public law enforcement officers. Tort law assigns responsibility for injuries to the wrongdoer by requiring the payment of compensation.

In the 1970s and 1980s, it was private attorneys general that uncovered numerous “smoking gun” documents in the asbestos product liability litigation. An industry-wide cover-up of the deadly consequences of unprotected exposure to asbestos dust, which destroyed the health of hundreds of thousands of American workers, was unmasked in asbestos products liability cases. Johns-Manville Corporation, for example, had definite knowledge as early as the 1930’s of the deadly consequences of unprotected exposure to asbestos dust but had a corporate policy of not informing employees that x-rays taken by company doctors revealed clear evidence of asbestosis.<sup>5</sup> Johns-Manville executives claimed that this policy was motivated by concern for employees so they “can live and work in peace and the company benefit by their many years of experience.”<sup>6</sup> The asbestos industry lulled government regulators into complacency for decades with false assurances that their products posed no health hazard.<sup>7</sup> More recently, private attorneys general have alerted the public to the danger of Firestone tires mounted on Ford Explorers. Women, have benefited from the work of private attorneys general who exposed the hazards of silicone breast implants, the Dalkon Shield intrauterine device, the Copper-7 birth control device, DES, and super-absorbent tampons. All Americans will benefit from a strong law in cyberspace where there is no shortage of wrongdoing undetected by authorities.

### **Why is tort law necessary in cyberspace when there is a criminal law with greater penalties?**

Criminal law does play a key role in enforcing laws or norms against child pornography, online gambling, and computer abuse. However, the law reporters reveal few cases where criminal prosecution has played a significant role in protecting individuals against invasions of privacy, online harassment, or the havoc caused by computer viruses such as Red Code or Melissa. We argue that there is inevitably an enforcement gap because of the rapidity of technological change. Before the criminal law can be mobilized, wrongdoers must have received clear notice of the elements of a crime to comply with due process requirements. Criminal statutes simply cannot keep pace with the rapidly changing technology. The difficulty of prosecuting cybercrimes is illustrated by the first Internet criminal case of *United States v. LaMacchia*.<sup>8</sup> David LaMacchia, an MIT student, was prosecuted for permitting online users to download copyrighted software programs at his Cynosure bulletin board. Pseudonyms and encryption

---

3 *Associated Industries v. Ickes*, 134 F.2d 694 (2d Cir. 1943).

4 *Id.* at 704.

5 *Janssens v. Johns-Manville Co.*, 463 So.2d 242 (Fla. 1984).

6 *Id.*

7 *Prudential Ins. Co. v. United States Gypsum*, 828 F. Supp. 287 (D.N.J. 1993).

8 871 F. Supp. 535 (D. Mass. 1994).

were used to conceal this activity. The criminal action against David LaMacchia was ultimately dismissed because the federal court held that the criminal penalties of wire fraud could not be imposed because there was no proof that LaMacchia had received any financial gains or profits from the infringing acts of illegal copying. The government was unable to prosecute the defendant because the statute was designed for a conventional criminal with a financial motive. It was not until the end of 1997 that the *No Electronic Theft Act of 1997* eliminated the LaMacchia loophole (NET). Criminal law inevitably lags behind the rapidly evolving Internet. The remedies of tort law such as conversion or trespass to chattels are more flexible tools that can apply ancient principles to new technologies.

We argue that tort remedies will fill an enforcement gap in cyberspace especially where law enforcement agencies have yet to address high tech issues. Tort law supplements but does not supplant the work of federal and state agencies whose task it is to protect the public interest. Tort remedies are more flexible than criminal law and can be updated to apply to cyberspace. Tort law has no death penalty or ability to incarcerate a defendant. Criminal justice agencies lack the computer resources and expertise necessary to detect and prosecute cybercrime. The FBI does not have the tools necessary to counter worldwide terrorists who communicate through the Internet. If tort law developed a duty to report known terrorist activities at web sites, it would be helpful to law enforcement. The cutting edge of Internet duties will be the question of whether web sites have a duty of due care to protect Internet security.

The sting of the remedy of punitive damages is civil punishment in the form of monetary damages proportional to the wealth of the defendant. Tort remedies adapted to Internet wrongdoing will play an increasingly important role in punishing and deterring fraud, hacking, and other wrongdoing on the Internet. In each case, tort law, rather than criminal law, has protected cyberspace consumers and users. By the time a criminal statute can be enacted to counter an Internet-related threat, the creative cyber-criminal finds new technologies to bypass an essential element of the prohibited act or offense.

### **What are the most common types of cyberspace torts being committed in recent years?**

Old torts are already being adapted to Internet-related wrongdoing to deter online harassment, spam e-mail, invasions of privacy, and hate speech that goes unpunished by the public authorities. A doctor won a \$675,000 libel damages award for a false charge that he was accepting kickbacks on a Yahoo! message board.<sup>9</sup> Plaintiffs are successfully using John Doe subpoenas to unveil anonymous wrongdoers on the Internet.<sup>10</sup> Private enforcement or a greater role for e-cops is needed to fill the inevitable enforcement gap in a rapidly evolving information economy.<sup>11</sup> In another case, a John Doe subpoena was used to unveil an anonymous poster who charged a physician with underbidding on contracts for Emory University's Pathology Department.<sup>12</sup>

### **Do you foresee any new types of cyberspace torts developing as a result of advanced technology?**

It has been a long time since a new tort has emerged. The most recent tort is the intentional infliction of emotional distress that was first articulated in 1946 by American Law Institute's Restatement of Torts. California became the first state to recognize this cause of action in the *Siliznoff* case involving a union that hounded and threatened a non-union trash collector.<sup>13</sup> Over the past two decades, a few states have recognized the tort of spoliation of evidence punishing defendants who covered their trail by

---

<sup>9</sup> Margaret Cronin Fisk, Net Libel Verdict is Upheld, *The Nat'l L. J.*, (Dec. 25, 2000) at A19.

<sup>10</sup> John Doe subpoenas are to the Internet Service Provider and require the provider to disclose the identity of customers for anonymous Internet postings. *Id.*

<sup>11</sup> Law enforcement agencies have been slow to adapt to Internet-related wrongdoing. Michigan Governor John Engler recently proposed a Michigan state "cybercourts to address high tech issues." See Doug Isenberg, "The Pros and Cons of 'Cybercourts,'" (last visited Aug. 8, 2001) <<http://www.gigalaw.com/articles/2001/isenberg-2001-04-01.html>>.

<sup>12</sup> Margaret Cronin Fisk, "Net Libel," *Id.*

<sup>13</sup> *State Rubbish Collectors Ass'n v. Siliznoff*, 240 P.2d 282, 286 (Cal. 1952) (adopting Section 46 of the 1948 Restatement (Second) of Torts).

destroying or altering smoking gun records in medical malpractice or product liability cases. The spoliation remedy will need be updated because of the ease with which electronic records can be manipulated. Increasingly, the modus operandi of wrongdoers on the Internet involves pseudonyms and misuses of encryption. Section 870 of The Restatement of Torts proposed tort liability for defendants who intentionally injured to another and could show no justification or excuse, sometimes called the innominate or *prima facie* tort.<sup>14</sup> The innominate tort concept has not been widely adopted but may become necessary to punish and deter Internet torts. Online stalking, for example, does not fit neatly into the traditional tort of assault because it lacks the element of imminence. The plaintiff must demonstrate that she was in apprehension of an imminent battery to recover for assault. The innominate tort may be appropriate where traditional torts fail.

We are impressed with the innovative ways that traditional tort actions are used to confront new dangers. The ancient tort of trespass to chattels, which was originally employed to compensate for injuries to personal property, has been extended to intangible property interests in cyberspace. An ex-employee of Intel Corporation was found to have committed trespass to chattels by sending thousands of e-mails to current employees of the company.<sup>15</sup> His purpose was to form an organization of former Intel employees who have filed claims against the company. Intel ordered the former employee to stop sending spam e-mails to its employees. When the ex-employee continued sending messages, Intel charged him with trespass to chattels. The company argued that the ex-employee's unsolicited e-mails constituted a trespass of Intel's computer system.<sup>16</sup> The court agreed rejecting the former employee's First Amendment defense because there was no state action as Intel was a private corporation.<sup>17</sup> Criminal law is often powerless to counter great threats to individuals and companies.

Another expansion of trespass to chattels has been in restraining web crawling to extract data from their competitor's site, which is, in effect, a form of unfair competition. In *Register.Com, Inc. v. Verio Inc.*,<sup>18</sup> a register of Internet domain names, sought an injunction against a competitor enjoining the use of automated software robots in accessing and collecting registrant contact information contained in their database. The federal court issued a preliminary injunction barring the defendant from using its search robots to extract information from the plaintiff's web site. The court found that the defendant was trespassing on the plaintiff's site by violating the Terms of Use applicable to the database.<sup>19</sup> Trespass to chattels or conversion may apply in a computer virus depending on the substantiality of loss. Conversion would be appropriate if the entire computer system was irretrievably lost whereas trespass to chattels is appropriate for lesser intrusions.

Internet security is another area where tort remedies are urgently needed. In July of 2000, a hacker broke into the University of Washington Medical Center's internal network and downloaded computerized admissions records for four thousand heart patients.<sup>20</sup> The medical facility would be negligent in engaging in conduct if it failed to exercise reasonable care under all the circumstances. For example, if a hospital did not have adequate information security, it could be considered negligent. A hacker's motivation in that case was to document the inadequate information security that protects confidential patient information at the medical center. This incident raises the question of whether the victim of hacker activity may be liable for negligently securing their computer system. This section

---

14 Richard Wright, "Once More into the Bramble Bush: Duty, Causal Contribution, and the Extent of Legal

Responsibility" 54 Vand. Law Rev. 1071 (2001) (citing Restatement (Second) of Torts §870 cmt. 1 (1979)) Section 870; states that, "One who intentionally causes injury to another is subject to liability to the other for that injury, if his conduct is generally culpable and not justifiable under the circumstances." Restatement (Second) of Torts §870 cmt. 1 (1979).

15 Ex-Employee's E-Mails to Intel Workers Are Not Protected Speech, Judge Rules, 16 Comp. & Online Indus. Litig. R. 8 (May 18, 1999).

16 Id.

17 Id.

18 2000 U.S. Dist. LEXIS 18846 (S.D. N.Y., Dec. 11, 2000).

19 Id.

20 Kevin Poulsen, "Hospital Records Hacked Hard," Infowar.com, Dec. 07, 2000 <[http://www.infowar.com/hacker/00hack\\_120700a\\_j.shtml](http://www.infowar.com/hacker/00hack_120700a_j.shtml)>.

explores the potential liability of a website or computer system to third parties for permitting a hacker to invade its computer system.<sup>21</sup> Another closely related question beyond the scope of the paper is whether a software vendor would also be liable for marketing or failing to recall software with known vulnerabilities.<sup>22</sup> Tort law's remarkable capacity to adapt and evolve to meet new threats and dangers makes it an important institution of social control in cyberspace. A strong tort regime in cyberspace will teach Internet wrongdoers "tort does not pay."<sup>23</sup>

Remedies that adapt traditional tort law principles to Information Age harms and hazards are currently evolving to police new forms of misbehavior such as Internet fraud, on-line stalking, the invasion of privacy, and defamatory postings on web sites. For example, women have been targeted by cyberstalkers who are aided by Internet search firms that locate personal information about their victims. Men have harmed women by malicious postings on sadism web sites, by posting pictures of the female's face superimposed on a nude body, and by threatening them through e-mail. Tort law is frequently the only defense these victimized women have available. Similarly, torts have been used to punish those who use the Internet to recruit children for pornographic purposes. Tort remedies are essential because the criminal law often lacks the flexibility to deter and punish these forms of wrongdoing.

**In Defense of Tort Law** also identifies privacy-based torts as yet another expansion of traditional principles to cyberspace. Immunities enacted to limit the liability of America Online, CompuServe and other service providers for defamatory postings made by unknown individuals have been expanded by the courts to shield providers from liability for many cyber torts. This broad immunity has had unanticipated consequences of protecting web sites that may profit from wrongdoing though they are not the content provider. The recent case of *John Does v. Franco Productions*<sup>24</sup> was a lawsuit filed by intercollegiate athletes who were secretly videotaped by hidden cameras in restrooms, locker rooms, and showers. The videotapes were sold on a number of web sites that transmitted still images of nude or partially clothed athletes on the Internet. The case against Illinois State University for failing to notify the athletes of the existence of the tapes was dismissed on grounds of qualified immunity. The case against the web sites was immunized by Section 230(c) of the Communications Decency Act. Courts have greatly extended the impact of Section 230 by insulating defendants from an even greater range of tort-based lawsuits.<sup>25</sup> A strong argument can be made that a web site should have at least some responsibility for warning the public of known criminal activity. Immunity is breeding irresponsibility because web sites have no incentive or duty to protect web site visitors and the general public. In the wake of the World Trade Center bombing, a host of fraudulent web sites have been designed to gather donations under the pretense

---

21 Microsoft SQL Server Version 7.0 and Microsoft Data Engine (MSDE) 1.0 for example, permits unauthorized users "to execute shell commands" permitting hackers to access secured, non-published files. United States Department of Justice, NIPC Advisory 01-003, March 8, 2001 (last visited Aug. 18, 2001) <http://www.usdoj.gov/criminal/cybercrime/NIPCadvisory.htm>.

22 Microsoft, for example has advised the NIPC that there are serious vulnerabilities with its software that permits "malicious users to run system commands on a web site." *Id.* It is unclear whether Microsoft has a post-marketing duty to take prompt remedial measures beyond a simple advisory. Another open question is whether software license agreement provisions disclaiming the implied warranty of merchantability would cover known vulnerabilities permitting intrusions.

23 *Rookes v. Bernard*, (H.L. 1964) 1 All Eng. Rep. 367 (noting the deterrent role of tort law).

24 2000 WL 816779 (N.D. Ill. June 21, 2000) (holding that Internet Service Providers were immunized from tort lawsuits even where they participated in web hosting and web design activities); See also *Does v. Franco Prods.*, 2001 U.S. Dist. LEXIS 8397 (N.D. Ill., June 20, 2001) (certifying class for purposes of injunctive but monetary relief); *Does v. Franco Prods.*, 2000 U.S. Dist. LEXIS 9848, (N.D. Ill., July 12, 2000) (granting motion to dismiss University on grounds of qualified immunity and find that plaintiffs did not show violation of clearly established right when Illinois State University officials failed to inform them of videotapes made without their consent). *Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998)* (dismissing defamation case against America Online on grounds of Section 230 immunity despite the fact that columnist had a contractual arrangement with AOL to provide exclusive content); *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (dismissing all claims, based on immunity).

25 *Blumenthal v. Drudge*, cert. denied, 524 U.S. 937, 118 S. Ct. 2341, 141 L. Ed. 2d 712 (1998) (dismissing claim on Section 230 grounds in case involving defamatory postings); *Lunney v. Prodigy Services Co.*, 94 N.Y.2d 242, 250, 723 N.E.2d 539, 701 N.Y.S.2d 684 (1999) (finding that commercial online service provider not held liable on libel claim because it did not "publish" allegedly defamatory e-mail message).

of collecting money for the victims and survivors. Within an hour of the disaster, there were bulk e-mail campaigns promoting “bogus relief efforts.”<sup>26</sup>

The World Trade Center bombings illustrate the role that the Internet can play as an instrumentality for the commission of acts of terror. The Taliban is thought to have posted encrypted messages on pornographic chat rooms as a method of evading law enforcement surveillance.<sup>27</sup> One of the emergent issues is whether a web site should have a duty of care to provide a safe site or to report wrongdoing that comes to its attention. Tort law should be permitted to develop a duty of care where the public interest is at stake. No case law presently exists that requires web sites to report the use of web sites as an instrumentality of crime. One of the troubling trends in cyberspace tort law is pervasive impact of immunities. One of the most troubling aspects of tort reforms is that they may cripple tort law's deterrent message. Our argument in the last chapter of **In Defense of Tort Law** is that we need a strong regime of tort law to protect us against wrongdoing in the borderless world of cyberspace. The Internet has become a haven for cybercriminals because of the possibilities for instant wealth without detection or prosecution.

### **Tell our Readers About Your Background.**

Michael Rustad is the Thomas F. Lambert Jr. Professor of Law and Director of the High Technology Law Program at Suffolk University Law School. Prior to joining the Suffolk faculty, he worked as an associate for the Boston law firm of Foley, Hoag & Eliot. He was a clerk to the late William E. Doyle of the U.S. Court of Appeals for the Tenth Circuit in Denver where he assisted the judge on the famous case of *Silkwood v. Kerr-McGee*. He is the co-author of the **E-Business Legal Handbook** (Aspen Law and Business, 2001) and **The Concepts and Methods of Sales, Leases and Licenses** (Carolina Academic Press, 1999). He has authored numerous law review articles and books and teaches courses in Internet law, commercial law and tort law at Suffolk University Law School.

Thomas Koenig is a professor of sociology and a founding faculty member of the Law, Policy and Society doctoral program at Northeastern University in Boston. He has published widely on topics such as political contributions, social network and statistical methodology, interlocking corporate directorates, punitive damages law, legal education and hierarchy in the legal profession. He teaches courses in legal theory, sociological theory, and social policy.

---

<sup>26</sup> Brian Krebs, “Spammers Raise Money For Bogus 'Victims & Survivor Fund' Newsbytes, Sept. 13, 2001.

<sup>27</sup> Stanley A. Miller II, Data Protections on Internet May Have Helped Plotters; Encryption Software Could be Used to Keep Plans Secret, Experts Say,” Milwaukee Journal Sentinel September 16, 2001.