Lost data: The legal challenges
By George H. Pike*

Another day, another data breach, another lawsuit. On September 22, 2006, a lawsuit was filed against America Online over AOL's release of 19 million search requests affecting 650,000 subscribers. The suit was filed by three AOL subscribers as a class-action lawsuit where they would represent all of the victims of the release.

The AOL data breach is not the first such incident. In the September issue of *Information Today*, Phillip Britt reported that over 190 data breaches had been reported between February 2005 and June 2006. In February 2005, ChoicePoint reported that information on over 160,000 persons was leaked to criminals posing as legitimate businesses. In May 2006, a laptop computer containing access to over 26 million veterans and military personnel data was stolen from a VA employee's home. At least two class action lawsuits are pending over that data breach.

Congressional proposals

The VA, AOL and other lawsuits have only been part of the legal response. Congress has introduced at least 10 bills addressing data breaches and identity theft. Most of these bills would enhance criminal penalties for data theft, require additional safeguards on stored personal data, provide for quicker notification to consumers of data breaches, or give consumers greater ability to secure and protect their financial and credit data in the event of a theft. As of yet, none of these bills have been enacted and only a few have made it out of committee.

There is no question that the data breach and identity theft problems are real and growing. The Federal Trade Commission recently estimated that as many as 10 million Americans are the victims of some form of identity theft each year. The cost of this theft is further estimated at over $50 billion to U.S. businesses and an additional $5 billion in out-of-pocket expenses. Consumers are asking, why can't the law protect them from this problem?

The answer, unfortunately, is that at the law can and does only go so far in protecting against data breaches and identity theft. Many of the reported data breaches are the result of criminal activity. In the ChoicePoint case the data was obtained by criminals through fraud. In the VA case, a laptop was stolen in what likely was a typical break-in with the thieves not targeting or even knowing that they had personal data. Hacking, phishing and other forms of information theft are already criminal offenses. The law is able to protect data only to the extent that people respect the law.

Another part of the challenges of the legal response is that it is the owner of the data–ChoicePoint or the VA–who is the "victim" of the crime. Data thieves are caught and prosecuted, and may be fined, imprisoned, and/or required to pay restitution. But any restitution would go to the data owner, and not necessarily to the people whose information was stolen.

Filing a lawsuit

For those persons, the civil justice system is the main remedy available. Lawsuits filed against ChoicePoint, the VA, and AOL (whose data breach was not caused by criminal action) are based on a combination of claims, most typically negligence, breach of contract, or in the case of the VA, violation of existing federal data security laws.

The negligence claim is the most common and tempting, but also can be very difficult to win. In a negligence claim, the victim–in this case the person whose data was compromised–must show four elements: a duty of care by the data owner; a breach of that duty; an injury to the victim; and that the breach of duty was the main cause of the injury. A February 2006 case involving a breach of student loan data arising from a laptop theft illustrates the problems.

Negligence law typically rests on what a reasonable person would do. In finding in favor of the student loan data company the court held that the company had complied with both the law and its own privacy policies. The law did not require perfect care. It only required reasonable steps such as security policies, training in those policies, risk assessments, and other safeguards. The court also found that having the data on the laptop was necessary for the company to process the information, and that both the company and the laptop owner acted reasonably.

What is foreseeable

That the laptop was stolen was not a breach of duty because the theft was found to be not "foreseeable." Negligence law only protects against injuries that can be reasonably (there's that word again!) foreseen. A criminal action by an unknown person is generally not considered foreseeable. While simply watching the evening news tells us that crime is common, the court held that a specific crime against a specific person at a specific time is generally not considered foreseeable.

Finally, the victim must actually suffer an injury. Negligence law considers this to be an actual financial loss or damage, not the "threat of future harm." Under this principle, you must show that you have actually been a victim of identity theft, not that your data *might* have been or *could* be misused. If the actual cash damages from a data breach–which generally do not include the time spent resolving credit and other problems–are not very great, the costs of pursuing a lawsuit may outweigh them.

The claim against the VA may have more success. First, as Phillip Britt's article reported, the VA inspector general found that the VA had ignored previous data security warnings, had weak management, and "dealt with lax rules." This makes a stronger case that the VA had a duty of care toward the information it held and breached that duty. Second, the case has been filed as a class action lawsuit. Instead of one person trying to recover a few hundred dollars of actual damages, all potential victims are considered a single plaintiff, and the recovery for one is considered to apply to all. With 26 million potential victims seeking damages of up to $1,000 each, the potential $26 billion recovery (unlikely) becomes worth pursuing.

Federal Privacy Act

Third is a specific federal law that adds additional responsibilities to federal agencies that maintain databases of personal information. The Privacy Act of 1974 mandates that federal agencies create and maintain rules of conduct for the development, operation and maintenance of personal records. In addition, it requires safeguards against, "any anticipated threat or hazard" to the records. In storing the records on a laptop and taking the laptop home, the VA is alleged to have violated the Act by either failing to follow established procedures, or that the procedures do not meet the Act's requirements.

Unfortunately, the Privacy Act only applies to information obtained and stored by the federal government, such as military, tax, VA, and other records. It does not apply to private data providers such as ChoicePoint, AOL and Lexis.

Other federal laws, including the Computer Fraud and Abuse Act of 1984, the Electronic Communication Privacy Act of 1986, and the Identity Theft Assumption and Deterrence Act of 1998 do apply to private data providers and have strengthened criminal penalties for hacking and identity theft. However, they do not address standards for the protection of stored data. The Gramm-Leach Bliley Act of 1999 requires financial institutions to develop and implement data security program, and identify reasonably foreseeable risks to customer information. However, the Act only applies to financial institutions and does not specify what steps are required.

State laws

A number of states have passed laws requiring data companies to give their customers notice of any data breach. California has enacted several laws requiring notice of security breaches, restrictions on the use of Social Security numbers, mandating the destruction of customer records that are no longer needed, and allowing consumers to determine whether personal information is provide to third parties. But state laws only apply within the state's boundaries, and still don't mandate specific security rules or procedures.

Certainly the law can be strengthened. The Senate is considering the Identity Theft Protection Act which would extend the Privacy Act's requirements to anyone who maintains or uses personal information The Data Accountability and Trust Act is a similar bill in the House of Representatives. Both proposals would require stronger data protection procedures, better means for resolving identity theft credit problems, and stronger penalties for data theft–including theft from laptop computers. Both bills have been reported out of their respective committees but have not been voted on by the Senate or House.

Strict liability

Will these proposals–if enacted–be enough? While they may make U.S. based data thieves take notice, they will have little effect on data thieves operating outside the U.S., where much of the stolen data ends up. Some commentators have argued for an even stricter liability standard for data protection. If you have data and fail to protect it, you're liable. Period. Whether this is realistic is questionable.

Certainly something needs to be done. As I was about to compose this final sentence, my RSS news feed reported the theft of another laptop containing personal data on 50,000 people. Another day, another data breach.

*George H. Pike is the Director of the Barco Law Library and Assistant Professor of Law, University of Pittsburgh School of Law.