
Consumers' Right-To-Know: Maintaining Customers' Rights, Preventing Cyber Terrorism, and Preserving Banks as Part of Our Critical Infrastructure

Emily I. Perkins

George Mason University,
8270 Greensboro Drive, Suite 700,
McLean, Virginia, U.S.A.
e-mail: emily@johnperkinslaw.com

Emily Perkins graduated from George Mason University School of Law in 2003, where she was a member of the Moot Court Board, Delta Theta Phi and the Intellectual Property Law Society. Emily is currently a first year associate at Williams Mullen in the McLean, Virginia office.

INTRODUCTION

Terrorists of yesterday used to calibrate their violence and harm they caused to just the right amount to get the government to sit down at the table and address their political grievances. The terrorists of today no longer calibrate their violence, nor do they aim merely to affect the government. Today, terrorists' goal is to kill and destroy as much as they can; the new political objective is to create a theocracy.¹ They bring the threat to our shores: our airports, our cities, and even our banks. They aim to disrupt and destroy all aspects of our critical infrastructure to reach this new political objective.

America today must face this new objective by protecting our critical infrastructure and preempting any damage that terrorist activities could toll against this country. This means evaluating each aspect of our critical infrastructure and securing it from vulnerabilities to terrorist activity. No doubt, such a daunting task will take years, and with the constantly rapid change of technological advances in cyber terrorism, the task may never truly be complete. Nonetheless, if America is to preserve its liberty and the liberty of its citizens, we must face the new terrorist objective aggressively.

One such aspect of our critical infrastructure is the banking industry. The proper functioning of banks is vital to the proper functioning of the country. America's banking industry is comprised of private institutions, heavily regulated by the government, and yet remains incredibly vulnerable to terrorist activity using cyberspace. This paper discusses those vulnerabilities and suggests methods for protecting banks against cyber terrorism without

¹ Susan Spaulding, Lecture at George Mason University School of Law, Cyberterrorism and National Security Class (February 25, 2003).

unnecessarily impinging upon the rights of citizens and institutions within the banking industry itself.

We first begin with a discussion of how banks use the Internet, and how that use results in banking customers' vulnerability to cyber attack. Second, is a discussion of who should be responsible for preventing cyber terrorism, and whether customers should have the right to know when a hacker or possible terrorist has exposed their information, which is held in a bank database. Third, this paper evaluates current right-to-know laws and determines that since banks are not a government agency, it would be unconstitutional to apply traditional right-to-know law to the banking industry. Thus fourth, the paper explores several alternative solutions toward securing bank databases; namely, the institution of a reporting requirement that would enable the public to obtain information on incidences of hacking through a request made under the Freedom of Information Act. Fifth, since any legal topic relating to the Internet is largely undeveloped, this paper compares and contrasts the privacy issues faced by banks and Internet service providers to provide incite on the scope of privacy protection on the Internet. Sixth and last, this paper briefly discusses another possible solution to poorly secured databases, which is to broaden the scope of existing liability rules already applied to banks for the protection of all customers' information.

BANKS, THE CRITICAL INFRASTRUCTURE, AND CYBER TERRORISM

The Critical Infrastructure Protection Act of 2001 states that the critical infrastructure is comprised of "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."² Banks fit squarely within this definition of critical infrastructure. The banking industry is a system, both physical and virtual, that if incapacitated or destroyed would debilitate the economic functions of this country and the countries with whom we transact; thus an attack would have a debilitating impact on our economic security.

Banks maintain an accounting of monies for everyone from individual citizens and publicly held corporations to government agencies. A crippling of the banking system would disrupt all aspects of commerce, from seemingly inconsequential transactions, like buying lunch, to larger transactions such as purchasing a home, completing a corporate merger, or developing new military airplanes for the nation's defense. Banks maintain this array of accounts by relying heavily on electronic transactions made possible only through cyberspace. Most of this information is proprietary, private, and highly sensitive to disruption—the transactions simply cease in the event of an effective attack. The country cannot afford to fall victim to such a debilitating attack; thus, someone must insulate the banking industry from cyber terrorism.

² Critical Infrastructure Protection Act, 42 USC 5195(c) (2001); See also, The Patriot Act of 2001 § 1016e.

