

---

## 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.<sup>1</sup> 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

---

<sup>1</sup> 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."<sup>2</sup> 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.

---

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

## THE BANKING INDUSTRIES' USE OF CYBER SPACE

"In the last decades of the 20<sup>th</sup> century, computer technology transformed the banking industry. The wide distribution of automated teller machines ("ATMs")...[and]...[o]nline banking through the Internet...allow for electronic payment of bills, money transfers, and loan applications without entering a bank branch."<sup>3</sup> All of these transactions occur through the use of cyber space.<sup>4</sup> This technology revolutionized the banking industry, increasing their capabilities as well as their efficiency; but it also made their records vulnerable to intrusion from hackers with all types of intentions. Before the terrorist attacks of September 11, 2001, concern surrounding banks' vulnerabilities from the use of cyber space appeared minimal, and emphasis remained on the incredible conveniences cyber space brought to the banking industry and its customers. Today, concerns continue to grow, but most consumers take the security of their banking information for granted while databases of the banking industry remain largely available for intrusion.

Concerns about the security of databases in the banking industry should grow. On February 19, 2003, the Washington Post reported one of the largest intrusions of this kind. Eight million credit accounts were exposed when a hacker broke into a computer database of a company that completes credit card transactions.<sup>5</sup> The database contained account numbers and other financial information that could be used toward terrorist activity. More on point, the mere capability to hack into such a database is evidence of the increasing threat that cyber terrorism could successfully target and cripple American banks.

Such capability could cause debilitating chaos in America in at least three ways. First, in the event of a similar cyber attack, consumers' accounts would be frozen and they would have no means for conducting daily transactions, from acquiring food to eat, to making airline and hotel reservations. Second, consumers' private information would be in the hands of the hacker to use as [s]he sees fit. A hacker could use the information to track and terrorize individuals, steal identities and carry out terrorist activities in the consumer's name, or steal assets and use them to pay for terrorist activities. Armed with the conveniences of the Internet and millions of Americans' vital account information the possibilities for debilitation are great.

The third possibility for debilitating chaos is an event reminiscent of the historical run on the banks that resulted from the stock market crash of 1929. The cause for the 1929 incident was that consumer confidence was undermined when consumers suddenly gained knowledge that the bank did not hold enough cash for all account holders to withdraw all funds in their accounts, and there was a risk that others would withdraw funds, leaving someone who had "money in the bank" with no actual money.<sup>6</sup>

---

*Banking*, The Columbia Encyclopedia, 6<sup>th</sup> Ed. (2001), at <http://www.bartleby.com/65/ba/banking.html>.

Id.

Jonathan Krim, *8 Million Credit Accounts Exposed, FBI to Investigate Hacking of Database*, Washington Post, Feb. 19, 2003, at E1; See also, [www.cnn.com](http://www.cnn.com), *Root of Massive Credit Card Theft Found*, Feb. 20, 2003.

*Great Depression*, The Columbia Encyclopedia, 6<sup>th</sup> Ed. (2001), at <http://www.bartleby.com/65/gr/GreatDep.html>;  
*Panic*, The Columbia Encyclopedia, 6<sup>th</sup> Ed. (2001), at <http://www.bartleby.com/65/pa/panic.html>.

With the banking industry's failure to secure its databases while increasingly relying on the Internet, it faces the risk of a modern day recurrence of the 1929 run on the banks, because "[w]ithout data privacy protection, consumers may be reluctant to do business on the Internet."<sup>7</sup> If consumer confidence is undermined by the vulnerability of bank databases to cyber terrorism, and the banking industry relies heavily on the Internet to conduct transactions, then consumers will be reluctant to trust banks with their money. Thus, the banking industry must secure its databases against hacker and terrorist intrusion or the public's confidence will be undermined and the banking industry, consumers, and the country will suffer.

Luckily, this time news of the February 2003 database hack came quietly, it did not implicate the name of the company whose database was exposed, and it went almost entirely unnoted by the general public. The lack of information here may have preserved public confidence in the banking industry for now, but we cannot build the security of our country and its citizens on hopes that information, which undermines public confidence, be suppressed. That approach will fail the banking industry in the long run. Eventually, information seeps into the public conscience and the sustainability of our banks, a substantial part of our critical infrastructure, must be built on foundations that inspire public confidence. The right-to-know is one such foundation.

Nevertheless, the question remains, should consumers have the right-to-know if a hacker has exposed their banking information, when the banks and not the consumers own the databases? With the surmounting concerns about privacy on the Internet as well as identity theft, surely we would expect the answer to be a resounding "yes!" However, currently there is no legal requirement that banks inform account holders when the hand of a hacker has exposed a customer's private information. Account holders affected by the February breach were not notified. Thus, the answer to this looming question appears to be, "no." To be sure, something must be done to ensure banks can prevent hackers—terrorist or otherwise—from exposing their customers' proprietary information. Since banks, like 80%-90% of the country's critical infrastructure, are owned and operated by private industry<sup>8</sup>, there is another issue that must be addressed before establishing whether consumers have this right-to-know. That issue is to determine *who* should secure the banking industry from cyber terrorism? The three obvious options are banks, consumers, or the government.

#### WHO SHALL PROTECT BANKS FROM CYBER TERRORISM?

Who shall protect banks from cyber terrorism—banks, the government, or you? As explained in the previous section, the government heavily regulates banks, and banks are a key part of the

<sup>7</sup> McTigue, Deborah M., *Marginalizing Individual Privacy on the Internet*, 5 B.U.J. SCI. & Tech. L. 5, ¶ 41 (Spring 1999) (citing Peter Menyasz, U.S. Move to Privacy Legislation Seen as 'Inevitable' Over Long Term, 66 U.S.L.W. 2238, 2238 (Oct. 21, 1997), and quoting Professor Joel Reidenberg, *Frodham University Law School*; see also Ian Lloyd, *An Outline of the European Data Protection Directive*, J. Info. L. & Tech. 1996 (Jan 31, 2996) <<http://www.elj.warwick.ac.uk/elj/ji>>

<sup>8</sup> John McCarthy, *Lecture at George Mason University School of Law, Cyberterrorism and National Security Class* (March 25, 2003).

country's critical infrastructure. Naturally, this means that the government has a strong interest in preserving the security of the banking industry. The government might see a need for monitoring banking transactions, or accessibility of bank databases containing customer information. Such close monitoring might be considered an unnecessary intrusion into private industry, as well as into the daily financial lives of private citizens.

Moreover, the fact that the banking industry is privately owned and operated indicates that the private sector also has a large interest in preserving the security of the banking industry. Banks must have specific concerns regarding the protection of customers' privacy against both the government and terrorists. If banks fail to maintain the security of their databases, they will lose customers and fail to operate profitably. At the same time, banks themselves have an interest in preserving the integrity of private banking information from excessive government intrusion to protect their privacy and the privacy of their customers. Since competing interests exist with regard to protection of the banking industry, it remains unclear whether the government or the banks themselves should be responsible for erecting the requisite shields against cyber terrorism.

### CONSUMERS' RIGHT-TO-KNOW

Generally, right-to-know laws are applied against government agencies rather than private institutions. The purpose behind them is to protect consumers (or private citizens) by forging a path for the free flow of information, thereby creating some degree of transparency and accountability in the government's actions. Existing right-to-know laws are distinct from any that might exist in the context of the banking industry, because the right-to-know laws contemplated here would be applied to private institutions. Thus, traditional right-to-know laws may not be appropriate in this context.

We begin this section with an overview of basic laws governing banking, and then evaluate whether a right-to-know law should be imposed against private institutions in the banking industry, or if there is another, more appropriate path for establishing accountability in the industry. In short, the goal for sure is to establish banks' accountability to consumers (or customers) because that is the best way to ensure the security and integrity of these databases, which are currently alarmingly vulnerable to cyber terrorist attack.

### LAWS GENERALLY GOVERNING BANKING

The basic laws governing banking were established and applied well before the advent of the Internet. Nevertheless, these laws establish the metes and bounds between bank and customer for most aspects of the banking relationship. Since no specific right-to-know laws exist with regard to the banking industry and its customers, this section briefly outlines the laws most relevant to whether customers have an implicit right-to-know if their information has been exposed by a hacker or terrorist.

These laws can be divided into two categories: (1) laws describing ownership; and (2) laws describing duties. The first set, laws describing ownership, state that the bank owns the deposits a customer makes to his account, while the customer owns the account itself. Since a bank account—separate from its deposits—is merely a compilation of data, the customer may also own the data currently vulnerable to attack. However, thus far neither case law nor statute speaks directly to this point.

The second set of banking laws relevant to whether customers have an implicit right-to-know if their information has been exposed are laws detailing the respective duties of the customer and the bank. Banks have a general duty of good faith and ordinary care to its customers.<sup>9</sup> Surprisingly, that duty is limited in that “the fact that a bank is indebted to its account holders for the amount of funds deposited imposes no special duty of care for the safekeeping of funds on deposit.”<sup>10</sup> The only time a special duty of care arises is in cases where the bank has established an advisory relationship with a customer.<sup>11</sup> For example, the bank establishes an advisory relationship with a customer when it makes a habit of notifying the customer that one of its bank supplied insurance policies is about to lapse.<sup>12</sup> Similarly, the customer has no duty to spot a bank’s accounting mistakes made with respect to his/her account, unless the bank regularly sends statements to the customer.<sup>13</sup> Notably, the customer has the right to request information, but once a bank fulfills that request, the customer then has the duty to examine the information provided.<sup>14</sup> In short, the duties between bank and customer are established by both parties’ actions during their course of dealing.

Additionally, banks owe the same general duties a bailee owes to a bailor when customers deposit valuables in a bank safety deposit box, and when customers deposit funds using automatic teller machines (“ATMs”).<sup>15</sup> So, if a customer’s valuables or money is lost, the bank has a duty to replace the items or their equivalent value.<sup>16</sup>

Lastly, but perhaps most interesting and relevant to the discussion below, is the fact that most states require banks to “maintain the capacity to furnish legible copies of” account information requested by the customer. Banks are required to keep this information for at least seven years from the day they receive it. Since it is impractical to keep the information in any other form but electronic, states are essentially requiring banks to keep databases of customer account information. Furthermore, since the customer owns the account, and the bank owns the deposits, it may be that the customer has an ownership interest in the databases. In short, this rule of law is most interesting, because it may suggest that the databases vulnerable to cyber terrorism are owned, at least in part, by the banking customer; and thus, this law may give the customer a right-to-know if the database containing his/her account information has been exposed.

<sup>9</sup> 10 Am. Jur. 2d Banks and Financial Institutions § 729 (2002); 11 Am. Jur. 2d Banks and Financial Institutions § 890 (2002).

<sup>10</sup> 10 Am. Jur. Banks and Financial Institutions § 738 (2002) (This rule is consistent with the rule that a bank owns the deposits while the customer owns the account).

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> 10 Am. Jur. Banks and Financial Institutions §§ 743 & 747 (2002).

<sup>14</sup> *Id.*

<sup>15</sup> 11 Am. Jur. Banks and Financial Institutions § 1016 (2002).

<sup>16</sup> 11 Am. Jur. Banks and Financial Institutions § 1021 (2002).

## NO RIGHT-TO-KNOW: THE UNACCOUNTABILITY OF BANKS

Despite laws implying customer ownership of bank maintained databases, the customer has no established right-to-know if a hacker or terrorist has exposed his or her account information, and so banks are directly accountable to no one.<sup>17</sup> This lack of clarity in the laws brings about a lack of accountability. Banks maintain databases comprised of private customer information, and if exposed by a hacker or terrorist it can have debilitating effects on the customer personally, as well as the country as a whole. Yet these databases remain vulnerable to cyber attack. The reason for this is that the customer has no established right-to-know if his or her information has been exposed; and thus, the banking industry is not accountable for its failure to secure consumers' account information, and the databases remain unsecured.

Perhaps consumers should have the right-to-know, because such a right makes banks accountable for security breaches. In other words, a consumer's right-to-know would give banks the incentive to secure their databases. Here, banks are the least cost avoider—they can secure their databases most cost effectively because they have the specialized knowledge about the databases that the government does not already have. On the other hand, establishing a customer's right-to-know might also serve to expose customers' private information—a result that benefits no one. Whether we need to establish a customers' right-to-know law against the banking industry will be discussed below. The paramount point is that the ultimate goal is to insulate databases from cyber terrorism, and a right-to-know law is merely one way we might accomplish this goal.

### THE PROBLEM WITH THE RIGHT-TO-KNOW: A DELICATE BALANCE

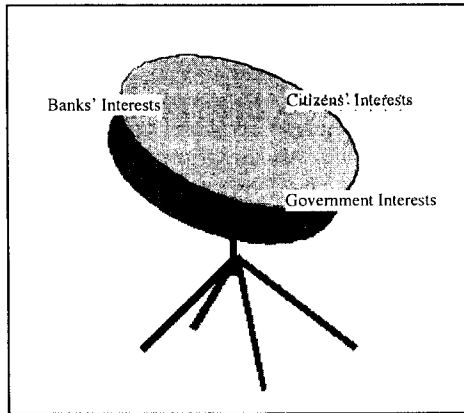
The problem inherent in any right-to-know law is that the Constitutional rights of several parties must be balanced, and thus, some rights must be strengthened at the expense of other rights. In the context of the banking industry, these rights are particularly difficult to balance. First, the interests of the government to preserve the banking industry as part of our critical infrastructure must be weighed against banking institutions' right to conduct business. Second, the rights of consumers to maintain some degree of privacy in their financial information from the government must be weighed against the government's interest in protecting private individuals from terrorism.<sup>18</sup> Third, customer's rights in keeping financial information private from fellow citizens must be balanced against the need for disclosure to protect national security.<sup>19</sup> Balancing

<sup>17</sup> They are only accountable indirectly when a customer's account is used, and then only if the customer can prove it, or the bank chooses to assume liability for it. See generally, 10 & 11 Am. Jur. Banks and Financial Institutions all sections (2002).

<sup>18</sup> Also, The Gram-Leach-Bliley Act, was submitted with the primary purpose of protecting the privacy of individuals' financial information, especially when it is in electronic form. Gramm-Leach-Bliley Act of 1999, H.R. 106-434, 106<sup>th</sup> Cong. (1<sup>st</sup> Sess. 1999).

<sup>19</sup> In fact, financial information has already been deemed as information that should be protected as private information. See, e.g., Public Information, Attorney General's Memorandum on the Public Information Section of the APA, Administrative Law Scope, (MB 2-7A 2003) (Stating that information concerning financial

all these interests at once is akin to balancing a single disk atop a pole; if one interest is given more weight, the disk will tilt away from all other parties. Indeed adequately balancing such interests that are so complexly related is a difficult task. Figure 1 is included below to help illustrate the delicate balance sought in maintaining customers' rights, preventing cyber terrorism, and protecting banks as part of our critical infrastructure.



*Figure 1:* Illustration of the delicate balance between customer and bank rights and the need to protect the critical banking infrastructure.

The problem in its simplest terms is that the party—whether bank or government or individual citizen—forced to reveal information is also forced to surrender a large degree of its privacy. In other words, the right to know of one party necessarily impinges another party's right to keep information private. In the typical context where right to know laws are applied the party required to make a disclosure, and thus surrender its privacy, is usually the government. Other than its duty to preserve national security, the government has no right to privacy in particular.<sup>20</sup> Thus, when the government is the subject of a right-to-know law, individual privacy rights are less of an issue.

However, where the disclosing party is a private institution, such as a bank, issues of individual privacy loom large. In the banking context, information sought through forced disclosure is the financial information pertaining directly to banking customers, or individual citizens. For this reason, the right to privacy enumerated in the United States Constitution precludes a blanket right-to-know law applicable to banks, lest individual citizens' right to privacy be impinged.<sup>21</sup> Since a right-to-know law as applied to the banking industry would be unconstitutional, we must seek another mechanism to achieve a higher standard of security in bank databases.

institutions is exempt from disclosure because it is important to "insure the security and integrity of financial institutions, for the sensitive details collected...if indiscriminately disclosed, [could] cause great harm.").

<sup>20</sup> The government only has a duty to keep information secret to preserve national security.

<sup>21</sup> U.S. Const. Amend. I.

Indeed, the balance between right-to-know and right to keep private is always a delicate one. But when the disclosing party is a private institution, rather than a government agency, the balance becomes even more delicate, because the interests being balanced are inherently distinct. On the one hand, the balance of the government's right to keep secret and the individual's right to know is somewhat simple to keep, because on both sides of the equation the goal remains the same—to preserve liberty. On the other hand, the balance is much more difficult to strike when neither party is the government. Necessarily, one party's rights will be enjoyed at the expense of the others. For example, a right to know law would, by definition, require banks to open information about its daily activities to its customers. Banks' records of its daily activities are comprised of its customers' private financial information. Opening these records to other citizens, and possibly the government, would expose citizens' private information to the public as well as the government. This kind of exposure is a violation of individual privacy, but such a disclosure no doubt would allow the receiving party to enjoy its right-to-know. Since the balance between right to know and right to keep secret is more delicate in this context—where neither party is the government—we must consider alternative methods for preserving the right to know.

### GIVING CONSUMERS KNOWLEDGE WITHOUT A RIGHT-TO-KNOW LAW

Since maintaining a Constitutional balance of rights appears impossible in the context of right-to-know laws against the banking industry, we must seek alternative methods for ensuring the security of bank databases. Toward that end, this section evaluates right-to-know laws as they exist in other contexts, as well as alternative methods by which consumers might obtain necessary information. Namely, this section first considers a tool already in place—The Freedom of Information Act (FOIA)—that could be used to increase the public's knowledge of the exposure rate of their private information, as well as banks' accountability for the security of the databases that contain such information. Second, we consider an analogy between Internet Service Providers (ISPs) and banks, whose problems with customer privacy are intriguingly similar. Third and last, this section evaluates the use of liability rules to provide banks the incentive to secure their databases against cyber terrorism.

### EXISTING RIGHT-TO-KNOW LAWS

All states have right-to-know laws,<sup>22</sup> and there are federal right-to-know laws governing federal agencies as well.<sup>23</sup> These laws include three basic elements: (1) presumption of a public right of access to government records; (2) enforceability of this public right in court; and (3) statutory

<sup>22</sup> Richard A. Bumstead, *An Unfettered Press: The Right to Know* at <http://usinfo.state.gov/products/pubs/press/press03.htm>.

<sup>23</sup> See e.g., *The Freedom of Information Act* 5 USC 552 (2003).

exemptions to disclosure of certain information.<sup>24</sup> The government bears the burden of proof that something is exempt from disclosure.<sup>25</sup> As mentioned above, most right-to-know laws are enforced against governmental agencies. For example, any records created during the Food and Drug Administration's (FDA) normal course of business are subject to disclosure to any requesting member of the public. Thus, if there is a question regarding the FDA's approval of a genetically altered vegetable, the documents and transcripts relating to that approval can be reviewed by a reporter or any other member of the public.

Moreover, some agencies respond to right-to-know laws by voluntarily providing information. The Environmental Protection Agency (EPA), for example, voluntarily provides information on their web site about chemicals to which Americans might have been exposed.<sup>26</sup> The government does not require such information be offered, but the EPA voluntarily provides it "in the spirit of the right-to-know laws."<sup>27</sup> Hence these laws encourage transparency in the transactions of government agencies, and they also hold the responsible agency accountable for its own actions. Such transparency and accountability is something the banking industry needs if it is to avert any activity that attempts to disrupt its normal operation.

#### THE FREEDOM OF INFORMATION ACT (FOIA): AN UNTAPPED RESOURCE

In practice, when documents are available under the FOIA, any private, or sensitive information is redacted. This allows information to reach the public, while maintaining individual privacy rights, as well as protecting interests in national security. There are at least two conceivable ways to use the FOIA in the context of the banking industry. First, the industry could be treated as if it were a government agency; this would require almost all of its records to be subject to disclosure upon a FOIA request. Since this essentially amounts to a right-to-know law against the banking industry, and as discussed in the previous section, such a law is almost certainly unconstitutional, this use of the FOIA is not recommended.

The second conceivable way the FOIA might be useful in the context of the banking industry is recommended. That is, to impose a reporting requirement on all entities within the banking industry. If banks and the entities they use, such as companies that complete credit card transactions, are required by law to report any breach of the security of their databases containing customer information, the consumer's right-to-know would be properly balanced with the many rights of privacy at issue. In practice, the reporting requirement would work as shown in Figure 2).

The most likely requester of information under the FOIA would be a reporter, who in turn disseminates the information through the press. This solution seems the best overall method of

<sup>24</sup> Richard A. Bumstead, *An Unfettered Press: The Right to Know at* <http://usinfor.state.gov/products/pubs/press/press03.htm>.

<sup>25</sup> *Id.*

<sup>26</sup> *Where You Live, Right to Know*, at <http://www.epa.gov/epahome/r2k.htm>.

<sup>27</sup> *Id.*

