

For more information visit:

[www.toraw.org](http://www.toraw.org)  
[www.zazona.com](http://www.zazona.com)  
[www.techsunite.org](http://www.techsunite.org)  
[www.hireamericancitizens.org](http://www.hireamericancitizens.org)

## The Programmers Guild Legislative Fact Sheet

[www.programmersguild.org](http://www.programmersguild.org)

### Information Technology (IT) Disclosure Act

Today, with terror alerts, war, and risks from abroad, homeland security is a major concern. But homeland security goes beyond fighting terrorist attacks -- it also entails keeping our country's data and our citizens' data secure. Under the Freedom of Information Act, consumers have the right to know who is viewing and managing their personal information. Consumers also have the right to move their assets to another institution if they feel their personal data is at risk or can be compromised.

A checking account or credit card is an ongoing relationship -- once you give a corporation your financial or personal information, they have it forever. When consumers entrust their financial or personal information to an institution they must rely on that institution to ensure the continued safety and privacy of that information. For this reason, consumers should have full disclosure about the location of their data and the personnel servicing it.

When an institution relinquishes support of its information technology (IT) processing or other operations offshore to foreign nationals, it should be mandatory to inform the consumer of this action. The institution should be required to mail a notice to consumers informing them that their data is being processed, manipulated, and viewed abroad. Our current manufacturing law requires that manufactured goods must state the country of origin of the product. This law ensures that consumers can exercise their right to "Buy American." For this reason, the law should be expanded to include a "*Serviced in*" notification label.

While many U.S. corporations have gone to great expense to secure, encrypt, and otherwise protect their vital customer and corporate data, they have also chosen to send the support and maintenance of some of these key systems overseas. The implications are alarming.

The Programmers Guild proposes the **Information Technology (IT) Disclosure Act** legislation to extend consumer rights for the marketplace of the 21<sup>st</sup> century. It will help ensure that consumers get the information they need in order to exercise choice, get redress or remedy, and protect the security and safety of their personal information.

#### **Consumers have the right to know:**

- if any data pertaining to their financial or personal well-being is being outsourced, maintained, processed, or viewed in a foreign country;
- the true identity -- as well as the city, state, and country -- where a customer service employee or call center employee is located if that person has access to any financial or personal information; and
- the citizenship of the person managing, viewing, or servicing the consumer's personal data.

#### **Consumers have the right to:**

- prevent their financial, personal, credit, and identification information (e.g., Social Security number, address, date of birth, credit card number) from being sent to any foreign country without their explicit written permission ("Opt-In");
- have their call to a service center or call center re-routed to the country where they are calling from; and
- have a "*Serviced in*" label appended to every statement mailed to them, including bank account statements, mortgage statements, credit card statements, stock and mutual fund portfolios, insurance information, and any other statements that contain financial or personal information.

#### **What are corporations doing with your personal information?**

- Major corporations are accelerating the movement of information technology, back-office operations, call center, and other white-collar service jobs to foreign countries. This offshore outsourcing of jobs is justified as a cost-saving measure, but is being done with little regard for the security of the data accessible by the people in these jobs.
- These services often are handed over to the lowest bidders in countries such as China, India, Pakistan, Vietnam, Russia, and other members of the former Soviet bloc. Some of these countries do not have congenial political relations with the United States government. Many of these countries may not be safe havens for our financial data and our country's future.

### **Why must Americans be concerned about *how* our information is being stored, viewed, and processed... and by *whom*?**

- Critical financial and personal information is currently being viewed, managed, and manipulated by software that is supported overseas. This process puts individual checking accounts, credit cards, and financial and personal information at risk. A consumer's life history is now easily accessible to foreign nationals and their governments. Given enough access, foreign governments can effectively hold our data hostage. The staff supporting this data and software is thousands of miles away, often cannot be extradited, and (in extreme cases) may harbor a deep hatred of America.
- In the United States, it is not uncommon for financial institutions to have potential employees bonded, fingerprinted, and drug-tested before hiring. With the advent of globalization, many jobs formerly performed by employees are being outsourced to offshore contractors. The workers at these offshore companies are not employees of the U.S.-based company that outsourced the job, and are not always subject to the same hiring standards (nor the same stringent laws) enforced in the United States.
- Experts have urged that our computer systems are vulnerable to hackers and cyber-attacks. Even though the physical data may be protected, the software is what makes the data "work." Encryption, decoding, and processing of data are all done via software run by IT personnel. To properly maintain this software, IT personnel usually require extensive access to critical data and, thereby, obtain an unprecedented level of control over the data.
- Data theft and/or terrorists attacks against our data are very real threats. It's happening already, and as more and more information flows overseas, such threats are likely to increase. A person with the right information could transfer money from someone's savings or credit card account to his own. Money could be stolen from American citizens' accounts and used to fund terrorist or other criminal activities.
- Current IT security relies heavily on catching the perpetrator after the fact. This is a deterrent for normal criminals, but not for terrorists. Suicide bombers have little concern about "capture" after committing the crime. Similarly, the only real deterrent for cyber-terrorism is prevention... and the first step toward prevention is keeping data and processing software within American control.
- Using programmer-maintained software, systems can be modified to route funds to other accounts, or to distort the values of data being presented or reported. Such changes can be implemented in such a clandestine manner that they easily defy detection. If a terrorist group wanted to know the names and addresses of customers who have more than one million dollars in bank accounts, a programmer could write a simple program to extract that information from the system without anyone ever knowing that the data had been accessed. In certain cases similar to computer viruses, the disruptive code may sit idle until a specified time or event triggers its execution.

Information is power, and information is stored as data that is manipulated by software. Ultimately, whoever controls the software will control the data... and can threaten our country's security. *The United States must not let corporations relinquish support of software and data critical to our nation's future.*