



*"The Perfect Fit for
Your Business"™*

ROBERT H. CARPENTER, JR.

ATTORNEY AT LAW
5912 CASTLEBAR LANE
PLANO, TEXAS 75093

—
TELEPHONE 972.473.4834

—
email: carpelaw@ix.netcom.com

May – June 2006

The Government Data Grab

The Fourth Amendment to the U.S. Constitution protects the people from excesses of the Federal government:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹

(The Supreme Court has applied the Fourth Amendment to state governments by incorporation based on the Fourteenth Amendment.)

Without devoting too much space to Constitutional law, one must note that the people are protected only from *unreasonable* searches and seizures. Thus, U.S. courts have found numerous exceptions, like that for the arrest of a fleeing suspect. Also, courts have interpreted the Fourth Amendment to require that a person must have a reasonable expectation of privacy in the place to be searched.

No doubt, the Federal government's interest in the data of U.S. businesses has not escaped notice. The National Security Agency (NSA) has tapped Americans' international telephone calls and developed a huge database of their calling habits (the latter obtained from American businesses just for the asking); the Treasury Department has monitored the international settlement of banking transactions; the Transportation Security Administration (TSA) has requested (and gotten from some airlines) data on the travel habits of Americans. No one yet knows the extent of the governments' interest in business data as they seek to combat terrorism and ensure domestic security.

And, governments' interest in data from financial institutions and their outsourced service providers pre-dates 9/11. State and Federal governments have long been interested in financial information for the collection of taxes and the prosecution of crimes.

¹ U.S. CONST. amend. IV.

Data Mining

Any business with half an ounce of marketing savvy knows the value of “mining” data for information that will drive sales and revenues. Governments now have finally turned to this technique in pursuit of their functions.

Of course, there are costs for American businesses. The advent of the *Gramm-Leach-Bliley Act*, the *Sarbanes-Oxley Act* and the *USA Patriot Act* – to mention only a few – has and will cost business and ultimately the consumer.

Subpoenas

Most businesses are familiar with subpoenas. They are issued by grand juries investigating possible crimes; they are issued by courts in furtherance of civil cases; they are issued by State Attorneys General (sometimes called civil investigative demands). The person on whom a subpoena is served is obliged to determine whether she has any of the items identified in the subpoena and make them available to the requester.

Under §215 of the *USA Patriot Act*,² the FBI can get a subpoena in connection with a terrorism investigation with very little effort, and keep it quiet for a year or more. There is little effective judicial review, and little chance for public scrutiny of the government’s actions.

National Security Letters

An even more secretive data gathering technique, actually around for many years but now more formalized under §505 of the *USA Patriot Act*,³ is the National Security Letter (NSL). Senior FBI officials are authorized to issue NSLs that demand information from the persons to whom they are issued without the oversight of a prosecutor or a court. And, there is a permanent gag order against disclosing the fact of the letter’s having been issued.

Search Warrants

If all of this does not make American business squirm, there is the search warrant, issued by a court usually at the request of a prosecution official. While search warrants are most often thought of in connection with criminal investigations and prosecutions, they are used, among other things, to enforce tax obligations.

Business Costs

Financial services companies keep a lot of data, on their customers and their financial transactions. Information technology outsourcers, particularly those in the financial services industry, have (at least temporarily) and keep (some for a long time) much of this same data. Financial services companies are reporting record costs in responding to voluntary and mandatory governmental requests for information to support not only the traditional regulation of banking, but also collateral purposes.

² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 § 215, 50 U.S.C. § 1861 (2000), *available at* http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001861----000-.html [hereinafter USA Patriot Act].

³ USA Patriot Act § 505, Pub. L. No. 107–56, 115 Stat. 272, 365-366 (2001) *available at* <http://f1.findlaw.com/news.findlaw.com/cnn/docs/terrorism/hr3162.pdf> (codified in scattered sections of U.S.C.).

One information technology outsourcer several years ago was served with a search warrant in connection with a tax collection inquiry. Mind, the warrant was obtained and served by a tax collection agency, not a criminal law enforcement agency. It authorized the tax collector to search a described data processing facility and to seize information about financial transactions that a suspected miscreant taxpayer had accomplished through one of the service provider's client banks.

Now, the information was commingled on thousands of rolls of microfilm with data from several other client banks. The data on the relevant microfilm covered periods of time not within the limits described in the search warrant and included data on thousands of other banking customers. Further, the requested data would likely consist of thousands of items among tens of thousands.

Rather than breaking down the door and seizing the relevant materials, the tax collector demanded that the service provider perform the research, segregate the data identified in the warrant, and turn over copies. The research time alone was staggering and would interrupt normal business operations that supported a large number of banks providing financial services to tens of thousands of people. Such an opportunity for overreaching is present in other data request forms.

Prevention vs. Cure

To reassure, the service provider refused to do anything other than what was required by the warrant – turn over hundreds of boxes containing thousands of rolls of microfilm – so that the tax collector could find what it was looking for. But, in the case of subpoenas or NSLs, that might not work. Remember, there is little if any effective review for those issued under the *USA Patriot Act*, and gag orders may prevent disclosure of their existence.

No doubt, service providers have not factored into their pricing models the costs of the ever-increasing demands by governments for data in their possession. For that matter, financial services companies probably have not either.

Both client and service provider are well-advised to review their contract and decide whether it properly allocates responsibility for data requested by means like those described above. Further, in crafting a contract provision to allocate this risk, the parties should address whether the allocation of risk will survive a termination of the outsourcing relationship and, if so, for how long. Finally, time limits to assert claims must be carefully examined and written because in some cases disclosure of the data request and the expenses related to it may be barred for years.

“An ounce of prevention is worth a pound of cure.”
– *Benjamin Franklin, Poor Richard's Almanack*

© 2006, 2007 Robert H. Carpenter, Jr.

This client newsletter is for informational purposes only, and is not intended to be legal advice. Transmission of this newsletter is not intended to create, and its receipt does not establish, an attorney-client relationship. Legal advice of any nature should be sought from legal counsel.

IRS CIRCULAR 230 DISCLOSURE: Notice regarding federal tax matters: Internal Revenue Service Circular 230 requires us to state herein that any federal tax advice set forth in this communication (1) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed by federal tax laws, and (2) cannot be used in promoting, marketing, or recommending to another person any transaction or matter addressed herein.