

# **The USA PATRIOT Act and American Business**

**WHAT YOU CAN DO TO PROTECT YOUR BUSINESS  
AND YOUR CLIENTS' PRIVACY**

# The PATRIOT Act and American Business

<b>THE PATRIOT ACT AND AMERICAN BUSINESS</b>	<b>1</b>
<i>Tangible Effects on Commerce</i>	1
<i>Costs to Business</i>	1
<i>Litigation Costs</i>	1
<i>Antithetical to American Business Values</i>	1
<b>PATRIOT ACT: WHAT BUSINESS NEEDS TO KNOW</b>	<b>2</b>
TITLE III: INTERNATIONAL MONEY LAUNDERING ABATEMENT AND FINANCIAL ANTI-TERRORISM ACT OF 2001	2
SECTION 215: ACCESS TO CUSTOMER RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT	4
SECTION 505: NATIONAL SECURITY LETTERS	5
2006 Reauthorization	5
OTHER LAWS AND POLICIES	6
Patriot Act Section 802	6
Executive Order 13224	6
Homeland Security Rules effective January 2009	6
<b>BUT DOES IT MAKE US SAFER?</b>	<b>7</b>
<b>RESISTING GOVERNMENT VIOLATIONS OF PRIVACY RIGHTS</b>	<b>7</b>
<i>Reef Seekers Dive Company, Beverly Hills, CA</i>	7
<i>Hotels and Casinos, Las Vegas, NV</i>	8
<i>Unnamed Internet Service Provider, New York, NY</i>	8
<i>Library Connection, Inc., CT</i>	9
<i>Qwest Communications</i>	9
<i>Internet Archives</i>	9
LESSONS LEARNED	10
<i>Consult a Lawyer</i>	10
<i>Do Not Submit Voluntarily to Demands</i>	10
<i>Challenge the Demand in Court</i>	11
<i>Notify Your Customers If Possible</i>	11
<i>Raise Your Concerns</i>	11
CIVIL LIBERTIES ORGANIZATIONS THAT PROVIDE LEGAL ADVICE	11

The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was passed in October 2001 as the Bush administration's response to the terrorist attacks on September 11, 2001. Proponents of the act described it as necessary to provide the U.S. government with the tools to combat terrorism. The law expanded the federal government's ability to conduct surveillance and detain suspects, increased the penalties for people convicted of terrorist charges, and enhanced strategies to prevent money laundering and other financial crimes. The act also enlisted businesses and financial institutions to gather an unprecedented volume of personal data from their customers. In early March 2006, controversial sections of the act that affected businesses were reauthorized with some changes; however, those changes did not go far enough to effectively protect businesses from unnecessary government intrusion.

## **Tangible Effects on Commerce**

The PATRIOT Act affects business in a number of ways. For one, it makes it more difficult for businesses to operate domestically and compete in an increasingly global market. It also imposes significant reporting and recordkeeping requirements on small and large businesses. These requirements have high costs which cut into businesses' profits, divert resources away from customer relations, and are of questionable use in fighting terrorism.

## **Costs to Business**

The PATRIOT Act forces businesses to share with the government private information about their customers' identities and transactions. Such requirements can discourage potential e-commerce customers, cause conflicts with foreign privacy requirements, and hurt relationships with customers.

## **Litigation Costs**

The act imposes higher litigation costs on businesses. Companies must defend against allegations of noncompliance, pay hefty fines if they are found noncompliant, and potentially defend against privacy lawsuits from customers. Here are two examples:

- Western Union and its parent company paid a settlement of \$11 million to the federal government in 2003 to resolve charges that the company failed to comply with provisions of the PATRIOT Act.<sup>1</sup>
- Since January 2006, AT&T has been fending off a class-action lawsuit by the Electronic Frontier Foundation (EFF) on behalf of customers whose data the company provided to the government without receiving a warrant.<sup>2</sup> Despite the July 2008 passage of the FISA Amendments Act, which granted telecommunications companies immunity for releasing private customer data without a warrant, EFF is continuing to pursue the lawsuit against AT&T, arguing that the FISA Amendments Act is unconstitutional.

## **Antithetical to American Business Values**

While the PATRIOT Act does create new concrete costs and liabilities for businesses, a more important problem is that its provisions are antithetical to the business values that enable American businesses to thrive: the free flow of information and ideas, minimal government intrusion, and the rule of law.

To grow, compete globally, and prosper, businesses must be free to explore and exchange ideas without strict and intrusive government regulations. They depend on the rule of law to establish a fair, open, and stable business environment. Under the PATRIOT Act, the government is more involved than ever before in even the most routine business transactions. With few or no controls on its actions, the government can act arbitrarily and unfairly punish businesses. The PATRIOT Act:

- Removes judicial review: government can act arbitrarily and interfere with business matters without justification.
- Increases government intrusion into business by adding new regulations and laws.
- Decreases or removes business and consumer privacy, hindering the free flow of information.

# PATRIOT Act: What Business Needs to Know

Three parts of the PATRIOT Act, in particular, hurt businesses:

- **Title III** imposes new reporting requirements and requires businesses to share more information with the government than was previously required.
- **Section 215** allows the government to subpoena any “tangible thing,” such as business records, and imposes on recipients a permanent gag order that bars, with very few exceptions, disclosure of the subpoena to anyone.
- **Section 505** allows the government to issue national security letters, a type of information request with no judicial oversight that is also accompanied by a gag order.

Business organizations, including the Association of Corporate Counsel; Business Civil Liberties, Inc.; the Financial Services Roundtable; the National Association of Manufacturers; the National Association of Realtors; and the United States Chamber of Commerce, wrote a letter to Senate Judiciary Committee Chairman Arlen Specter in October 2005 to request major changes to the above sections of the PATRIOT Act:

Confidential files—records about our customers or our employees, as well as our trade secrets and other proprietary information—can too easily be obtained and disseminated under investigative powers expanded by the Patriot Act. These new powers lack sufficient checks and balances.<sup>3</sup>

Although the influence of these business groups incited some PATRIOT Act reforms, many problems remain: the federal government continues requesting that businesses spy on their customers, violate privacy obligations, and comply with voluminous red tape requirements. This surveillance is of dubious value in focusing the government on actual terrorists and may, in fact, make the U.S. less safe.<sup>4</sup>

Further, the passage of the FISA Amendments Act in July 2008 granted immunity to telecommunications companies that share private customer records with the government without first receiving a warrant. This law’s constitutionality is still uncertain, leaving businesses open to litigation and their clients open to serious violations of privacy.

## ***Title III: International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001***

Title III of the PATRIOT Act, itself a separate act of Congress called the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, deals with financial crimes. Its intent is to prevent terrorists from illicitly obtaining funds for their activities.

In 2003, Congress significantly broadened the scope of the PATRIOT Act by redefining the term “financial institution” to use the broad definition included in the Bank Secrecy Act. This definition includes businesses such as travel agencies, pawnbrokers, car dealerships, jewelry stores, money changers, real estate companies, and, “[a]ny other business designated by the [Treasury] Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.”<sup>5</sup>

Having been expanded in this way, the PATRIOT Act now imposes increased reporting requirements on businesses that have never before had to track “suspicious activity,” significantly increasing their operating costs.

What Title III requires	What it means	How it hurts business
Greater “Due Diligence” <sup>6</sup>	<p>Affected businesses must:</p> <ul style="list-style-type: none"> <li>• Have an established anti-money laundering program in place.</li> <li>• Have a compliance officer and employee training program in place.</li> <li>• Check customers’ identities and cross check their identities against terrorist watch lists.</li> </ul>	<ul style="list-style-type: none"> <li>• Compliance with reporting requirements increases costs.</li> <li>• For small- to medium-sized businesses, which lack experience in due diligence, acquiring the needed expertise may be difficult and costly.</li> <li>• Failure to comply can lead to fines or criminal charges.</li> <li>• Reporting could discourage e-commerce by undermining the foundation of trust and respect for privacy central to e-commerce.</li> <li>• Businesses may prefer to collect less marketing data from customers to avoid having to hand that information over to the government.</li> </ul>
Increased Information Sharing and Reporting <sup>7, 8</sup>	<p>Affected businesses must:</p> <ul style="list-style-type: none"> <li>• Share suspicious or unusual transactions with authorities.</li> <li>• Notify authorities about transactions or accounts that are “red flagged,” possibly for something as trivial as a name similar to that of a terrorist.</li> <li>• Refrain from notifying customers that their data has been shared with the government.</li> </ul>	<ul style="list-style-type: none"> <li>• Undermines trust and customer relationships.</li> <li>• Compliance may create problems with foreign privacy laws, especially the EU Data Protection Directive, hindering global flows of people, ideas, and capital.</li> <li>• The definition of suspicious or unusual transactions is unclear. Businesses must choose between giving up too much information and facing government sanctions.</li> <li>• Failure to submit adequate information or to fully comply can lead to large fines or criminal negligence charges.</li> </ul>
Special Measures <sup>9</sup>	<p>Special measures are imposed when investigators feel that “reasonable grounds exist” to believe a transaction or account is of “primary money laundering concern.” There is no judicial oversight. When special measures are issued, businesses must:</p> <ul style="list-style-type: none"> <li>• Provide information to investigators, including the identities and personal information of all parties involved.</li> <li>• Comply with investigators’ requests for increased recordkeeping and information tracking.</li> <li>• Comply with orders not to open specific account types or engage in certain transactions.</li> </ul>	<ul style="list-style-type: none"> <li>• The lack of judicial oversight means that special measures could be used for purely political ends. In light of recent developments and historical trends, this is not an insignificant risk.</li> <li>• The government may interfere with legitimate business transactions.</li> <li>• Special measures are excessively strong: once the measures have been imposed, investigators can gain access to virtually all account records, past and present.</li> </ul>

## Section 215: Access to customer records and other items under the Foreign Intelligence Surveillance Act

The PATRIOT ACT Section 215 has attracted attention from civil libertarians because it provides the federal government with increased access to private records.

Simply put, Section 215 makes it easier for the federal government to demand customer records from businesses. To access customer records, law enforcement can now go to the Foreign Intelligence Surveillance Act (FISA) court and request a warrant. As long as law enforcement asserts that the records are “for an authorized investigation ... to protect against international terrorism or clandestine intelligence activities,” the judge must approve the warrant.<sup>10</sup> The customer need not be suspected of involvement in terrorism. The business that receives the warrant is subject to a gag order that bars the recipient(s) from revealing the information request to anyone, including the customer whose information the government sought. When the PATRIOT Act was reauthorized in 2006, the language was changed so that businesses are explicitly granted the right to discuss section 215 orders with legal counsel.<sup>11</sup>

Under Section 215, law enforcement may request any tangible thing from a business. This can include customers’ personal data, transaction records, account history, or possibly even genetic information.<sup>12</sup>

The changes made to the PATRIOT Act in 2006 do not effectively address business interests. Businesses continue to bear increased costs of complying with frivolous requests, expend management and labor resources for compliance, face increased legal costs, and risk undermining their relationships with customers. Furthermore, businesses’ ability to challenge requests is essentially meaningless, as they cannot be present at FISA court proceedings and the government often uses secret evidence to which businesses do not have access.<sup>13</sup>

Further, the FISA Amendments Act, passed in July 2008, grants immunity to telecommunications companies who provide private customer information to the government without first receiving a warrant, thereby making it more difficult for businesses to resist privacy-violating searches. The constitutionality of the act is still being determined through litigation, leaving companies open to lawsuits from customers whose information they share.

What Section 215 does	How it hurts business
<p>To obtain a 215 order, law enforcement must assert to a FISA judge that the requested information is related to an authorized terrorism investigation. Law enforcement does not need to provide probable cause that the customer in question is a terrorist suspect or is associated with a foreign power.<sup>14</sup></p> <p>When presented with a 215 order, a business:</p> <ul style="list-style-type: none"> <li>• Must turn over all requested customer information, including transaction records, personal information, account information, and account history.</li> <li>• May not notify the customer, the press, or anyone except legal counsel and the person retrieving the requested information.</li> <li>• May not be present in the FISA court to challenge the request and must instead file papers with the court. Government lawyers may argue their case in the FISA court and may use secret evidence to which the business and their counsel have no access.</li> </ul>	<ul style="list-style-type: none"> <li>• The lack of judicial oversight increases the potential for frivolous and counterproductive requests on the part of law enforcement.</li> <li>• Fulfilling such requests can impose significant direct and indirect costs on businesses.</li> <li>• Firms doing business overseas may come into conflict with foreign data protection laws which could result in higher legal costs, lost business, and damage to goodwill or brand reputation.</li> <li>• Firms could put themselves at risk of future lawsuits brought by customers whose data they have provided to authorities and by civil liberties, privacy, and advocacy organizations on their behalf.</li> <li>• Firms undermine both their ethical and contractual privacy obligations to customers and clients. Aside from potential litigation, this could lead customers to withhold data that firms rely on for marketing, customer service, retention, and general operations.</li> <li>• Firms face the potential loss of trade secrets and proprietary information.</li> </ul>

## Section 505: National Security Letters

The PATRIOT Act greatly expanded the scope and use of national security letters (NSLs), administrative subpoenas by which the FBI and other federal agencies can demand that businesses hand over certain customer records without any court supervision. NSLs received significant media attention in 2007 following the release of internal Department of Justice and FBI reports that revealed more than 1,000 violations, including civil liberties violations.<sup>15</sup>

Like section 215, section 505 has received much media attention due to its implications for privacy rights and civil liberties. Also like section 215, section 505 harms businesses. Before the PATRIOT Act, the government could only use NSLs when there were “specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power.”<sup>16</sup> As a result, they were infrequently used. The PATRIOT Act changed the law, allowing the FBI to obtain financial records, Internet and communication transaction records, telephone records, and other private records without having to show a connection between the records sought and a suspected terrorist.

NSLs can now be issued to any business as long as the requested data is relevant to an ongoing investigation. There is no direct judicial oversight, and law enforcement can request more types of records, including telephone logs, e-mail logs, financial data, bank records, credit reports, and customer data.<sup>17</sup>

### 2006 Reauthorization

Like Section 215, changes made to Section 505 during reauthorization are inadequate to protect businesses. Congress added language allowing recipients to discuss NSLs with legal counsel and to challenge the requests and gag orders in federal court.<sup>18</sup> While this is a step forward, businesses must still expend resources responding to and challenging NSLs.

These costs are particularly important in light of a March 2007 report by the Justice Department’s own Inspector General, which found frequent abuse of NSLs by the FBI.<sup>19</sup> According to the report, 159,700 NSL requests were made in 2003, 2004, and 2005. In 2000, before the passage of the Patriot Act, there were only 8,500 requests made. The report found that in a sample taken from 2003, 2004, and 2005, the FBI had abused these broad and unchecked powers 22% of the time. This is significant abuse, and businesses have suffered significant costs and financial penalties as a result of this big government intrusion. This abuse is the inevitable result of unchecked government power.

What national security letters do	How they hurt business
<p>To obtain an NSL, the FBI need only assert to the head of a branch office that the desired information is relevant to an ongoing investigation.<sup>20</sup> When presented with an NSL, businesses must either:</p> <ul style="list-style-type: none"> <li>• Provide the FBI with any requested phone or e-mail logs, financial data, bank records, credit reports, and customer data, or</li> <li>• Challenge the NSL in federal court.</li> </ul> <p>Furthermore, the recipient may not disclose that he or she has received an NSL except to legal counsel unless a federal court finds the gag order requiring permanent silence unnecessary. Businesses may not challenge a gag order until one year after a request.</p>	<ul style="list-style-type: none"> <li>• The lack of judicial oversight increases the potential for counterproductive and frivolous requests by law enforcement.</li> <li>• Businesses must take time and resources away from normal operations to collect information and provide it to law enforcement at their unilateral and unchecked discretion.</li> <li>• Complying with and challenging gag orders creates increased legal costs, lost business, and damage to goodwill or brand reputation.</li> <li>• Firms doing business overseas may come into conflict with foreign data protection laws which could result in higher legal costs, lost business, and damage to goodwill or brand reputation.</li> <li>• Compliance puts firms at risk of future lawsuits from customers whose data they have provided to authorities.</li> <li>• Firms undermine their privacy obligations to customers and clients. Aside from potential litigation, this could lead customers to withhold data that firms rely on for marketing, customer service, retention, and general operations.</li> <li>• Firms face potential loss of trade secrets or proprietary information.</li> </ul>

## Other Laws and Policies

Other post-9/11 anti-terrorist policies pose potential problems for businesses. Section 802 of the PATRIOT Act increases the government’s asset forfeiture powers.<sup>21</sup> Executive Order 13224 allows the executive to designate individuals “to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States.”<sup>22</sup>

Although these policies have the potential to be strong tools for fighting terrorism, their lack of judicial oversight makes it virtually impossible for a person, business, or organization whom the government has wrongly designated a “significant risk” or whose assets it has seized to appeal the decision. When the government makes this designation in error, a business may be crippled and unable to recover.

Policy	What it does	Risks
PATRIOT Act Section 802 <sup>23</sup>	<p>Allows the government to seize all assets:</p> <ul style="list-style-type: none"> <li>• Of individuals or organizations engaged in planning or perpetrating acts of terrorism against the U.S., or affording any person a source of influence over any such organization, or</li> <li>• Acquired or maintained by a person with the intent of supporting, planning, or concealing an act of terrorism against the U.S., citizens or residents of the U.S., or their property, or</li> <li>• Gained from, involved in, used, or intended to be used to commit any act of terrorism against the U.S., citizens or residents of the U.S., or their property.</li> </ul> <p>The government may seize assets based on the assertion of probable cause without prior notice or a prior hearing.</p>	<p>Because of the lack of judicial oversight:</p> <ul style="list-style-type: none"> <li>• A firm’s assets could be wrongfully seized, costing the firm financially or even bankrupting it.</li> <li>• A customer’s assets could be seized, depriving a business of money owed.</li> <li>• The assets of a business partner could be wrongfully seized, costing a firm financially and damaging its reputation.</li> </ul>
Executive Order 13224 <sup>24</sup>	<p>Allows the Executive, through the Treasury Secretary, the Attorney General, and the Secretary of State to designate an individual or organization a “significant risk.” After making such a designation, the Treasury Department blocks all property, finances, or property interests belonging to that individual or organization which come within the U.S.</p>	<p>Because of the lack of judicial oversight:</p> <ul style="list-style-type: none"> <li>• A firm’s assets could be wrongfully seized, costing the firm financially or even bankrupting it.</li> <li>• A customer’s assets could be seized, depriving a business of money owed.</li> <li>• The assets of a business partner could be wrongfully seized, costing a firm financially and damaging its reputation.</li> </ul>
Homeland Security Rules effective January 2009 <sup>25</sup>	<p>Instructs the Department of Homeland Security to “collect millions of new electronic records about private planes, imported cargo, foreign visitors and federal contractors,” including verification of employees’ legal right to work in the U.S., requiring private jet passengers to be checked against terrorist watch lists, and requiring companies “to submit detailed information about imported cargo 24 hours before it is loaded on a ship in a foreign port.”</p>	<ul style="list-style-type: none"> <li>• In testing, the database used to verify workers’ statuses contained incorrect information, which could prevent businesses from employing people legally able to work in the U.S.</li> <li>• If data collected by DHS, such as information about private jet flights or imported cargo, leaks out, business strategies could be compromised.</li> </ul>

## But Does It Make Us Safer?

Are these sacrifices worthwhile? Do the extra costs, increased labor, and increased government scrutiny actually result in greater security? Evidence suggests that they do not. Rather than increasing security, the PATRIOT Act has inundated law enforcement with useless data and has resulted in frequent abuse. To some extent, the regulations have made businesses less safe.

One limit on the PATRIOT Act's effectiveness is that it results in too much data. With increased reporting requirements, government agencies receive huge amounts of information. Sorting through it to find useful information is not only labor-intensive and cost-prohibitive, but virtually impossible. Law enforcement spends a great deal of time sifting through useless data and following up on false leads resulting from the flood of data about people with no ties to terrorism. The exorbitant amounts of data can make it harder for the government to zero in on real terrorists. This was a problem for law enforcement even before the PATRIOT Act, under the Bank Secrecy Act (BSA). According to an article by John Berlau,

While it did not cite the BSA directly, the [2003] joint Congressional inquiry report on intelligence lapses before 9/11 did find that law enforcement and intelligence agencies faced a "huge volume of intelligence reporting," within which were "various threads and pieces of information that, at least in retrospect, are relevant and significant." The report concluded that "although relevant information ... was available to the intelligence Community prior to September 11, 2001, the Community too often failed to focus on that information and consider and appreciate its collective significance in terms of a probable terrorist attack." This was partly because analysts were trying to find a needle in a very large haystack of data created by laws like the BSA.<sup>26</sup>

Numerous former government officials have also criticized the regulations:

- John Yoder, director of the Justice Department's Asset Forfeiture Office in the Reagan administration, said such programs are "highly counterproductive... It costs more to enforce and regulate them than the benefits that are received. You're getting so much data on people who are absolutely legitimate and who are doing nothing wrong."<sup>27</sup>
- Oliver "Buck" Revell, supervisor of the FBI's counterterrorism division in the 1980s and '90s has stated that "You can be buried in an avalanche of information. The total volume of activity makes it very difficult to track and trace any type of specific information."<sup>28</sup>

## Resisting Government Violations of Privacy Rights

The Federal Bureau of Investigation (FBI) issues over 30,000 national security letters (NSLs) each year.<sup>29</sup> These unconstitutional letters are not subject to judicial review and are accompanied by a gag order that bars recipients from ever discussing the nature of the FBI's demands with anyone other than legal counsel. Upon receiving these letters, many businesses simply submit to the FBI's coercion. Some may not be concerned with protecting their customers' right to privacy. Many more may believe that by resisting the FBI, they might make possible a future terrorist attack. Others may believe that they cannot challenge the use of an NSL. All of these beliefs, however, are wrong.

By acquiescing, businesses enable the U.S. intelligence community to occupy an ever more intrusive presence in our private lives. Our right to privacy is extremely important and should be protected. Fortunately, businesses can resist and challenge the government's unlawful attempts to invade our private lives, and doing so will not jeopardize the safety of our nation. The following are stories of courageous individuals and businesses who resisted.

### **Reef Seekers Dive Company, Beverly Hills, CA<sup>30</sup>**

In 2002, after the FBI successfully obtained information about all certified scuba divers in the United States from three private certification organizations, it went after information on diving-school dropouts. We know about that effort because Reef Seekers Dive Co., which offers recreational scuba diving classes, refused to cooperate with a federal grand jury subpoena requesting information on everyone who had started but had not finished one of its courses in the previous three years. According to the Electronic Frontier Foundation (EFF), which represented Reef Seekers, the FBI's

justification for the search was, in the absence of any evidence raising suspicion, to consider all such students potential terrorists who might carry explosives under water to blow up ships in a harbor.

Jeff Nadler of PADI, one of the three certification organizations that cooperated with the fishing expedition, claims to have cooperated with a verbal FBI request in order to avoid a subpoena. According to Cindy Cohn, EFF's legal director, PADI could have done the following in order to protect the privacy of the divers it had certified:

- Refused to cooperate until a subpoena was issued. Subpoenas are less likely to authorize "fishing expeditions" because they involve judicial oversight. In this case, a judge would have wanted information supporting probable cause of a crime or potential crime involving the persons whose records were sought.
- If a subpoena were eventually issued, notify the customers to seek court review, or challenge the subpoena. A civil liberties organization such as EFF would have offered free legal counsel.

## **Hotels and Casinos, Las Vegas, NV<sup>31</sup>**

In December 2003, the Department of Homeland Security (DHS) declared an orange alert in response to intelligence that indicated Las Vegas might be the site of a New Year's Eve terror attack. Determined to prevent an attack from occurring, but lacking solid information about the threat, the FBI launched a massive data-mining operation (under the leadership of Gervais Griff from the Proactive Data Exploitation Unit) that sought to collect information on everyone who would be staying in a hotel, renting a vehicle, leasing storage space, or entering the city by plane during the two weeks before New Year's Day.

When approached, many businesses quickly and unquestioningly complied with the FBI's demands for information. However, some did not. Most notably, the executives of many prominent casinos, such as the MGM Mirage, attempted to protect their customers' right to privacy by refusing access to their guest lists. When these casinos, and other Las Vegas businesses, refused to turn over the information demanded, the FBI began to use NSLs and grand jury subpoenas as a threat to force compliance. For example, FBI agents compelled many casino executives to turn over their guest lists voluntarily by threatening to use a national security letter to seek more sensitive information regarding their customers. In some instances, when even threats failed, the FBI followed through with their threat by issuing NSLs.

When New Year's Day arrived, the terrorist threat never materialized. The FBI's intensive and incredibly invasive data-mining operation failed to produce any credible leads and was subsequently terminated. Shortly later, the orange alert was dropped as well. Nevertheless, the vast amount of information that was swept up during the course of this investigation remains in FBI databases to this day.

## **Unnamed Internet Service Provider, New York, NY<sup>32, 33</sup>**

The *Washington Post* published, on March 23, 2007, an anonymous editorial from the president of a small internet service provider whose company had been targeted by the FBI. In this article, the unnamed CEO wrote that he had received, three years earlier, a national security letter from the FBI that demanded personal information about one of his customers. The NSL also contained a gag order that forbid him from discussing the FBI's demands, not only with the specific person whose information was targeted, but with anyone else. Under suspicion that the letter had not gone through judicial review, he contacted the American Civil Liberties Union (ACLU) and, subsequently, challenged the constitutionality of the NSL in court in April of 2004. Although the FBI dropped its demand later that year, the gag order remains. Consequently, to this day, he is unable to openly raise his concerns about the application of and secrecy surrounding national security letters.

The anonymous author of this editorial is still forbidden to discuss the nature of the FBI's demands. Nevertheless, he should be commended for his steadfast resistance because he never violated his client's privacy by giving to the FBI the personal information sought.

## **Library Connection, Inc., CT<sup>34, 35</sup>**

In July 2005, the FBI served George Christian, the executive director of the public library consortium Library Connection, with a national security letter and demanded access to all the usage records associated with a specific computer belonging to one of the consortium's libraries. Given the nature of Library Connection's computer system, however, complying with this demand would have required Christian to turn over the usage records for the entire patron database of the library in question. Beyond the exceedingly invasive nature of this demand, the NSL that Christian received was dated May 19, but was not delivered until July 13. Moreover, the NSL was issued in connection with an FBI investigation into an anonymous terror threat made nearly five months earlier by a user of one of the library's computers. Clearly, the threat was not a matter of national security. Consequently, Christian consulted with the executive board at Library Connection and decided to challenge the constitutionality of the NSL by suing U.S. Attorney General Alberto Gonzales.

Having made the decision to contest the FBI's use of the national security letter, Library Connection contacted the ACLU, which subsequently challenged, in August, the legality of the gag order that was associated with the NSL. In September, a judge ruled in favor of Library Connection; however, the FBI appealed the decision. The gag order remained in effect throughout the period that Congress was considering whether to renew the PATRIOT Act. Six weeks after the legislation was renewed, however, the FBI agreed to lift the gag order. By this time, it was too late for Library Connection to speak out to Congress and influence the debate over the legislation.

## **Qwest Communications<sup>36, 37</sup>**

When a May 2006 article in *USA Today* disclosed the existence of an enormous National Security Agency (NSA) secret program that involved collecting the phone records of millions of Americans and that aimed to "create a database of every call ever made" within the U.S., Americans learned that Qwest Communications was the only major telecommunications company that refused verbal requests to hand over its complete call records.

According to the article, this program, which was launched after September 11, 2001 in an effort to track suspected terrorists, involved analyzing the call records of millions of Americans to look for patterns that might indicate involvement in terrorist activity. The NSA successfully obtained, without warrants or the approval of the FISA court, the call records necessary for this program (known in the telecommunications industry as "call-detail" records) from the telecommunications giants AT&T, Verizon, and BellSouth (which collectively serve more than 200 million Americans). Although the phone call records that these companies willingly passed to the NSA did not contain their customer's most sensitive personal information (such as their names, addresses, and social security numbers), much of this information could easily be obtained by other means, if the NSA chose to do so.

Qwest Communications, long ridiculed for notoriously shoddy service, was reportedly the only major telecommunications company to refuse the NSA's unlawful request. When first approached, lawyers from Qwest raised concerns with the NSA about the legality of the request and worried about how the information they were being asked to provide might be used.

Despite heavy pressure from the NSA, Qwest demanded that the NSA take their request to the FISA court for approval. This did not happen. Eventually, unable to reach an agreement that satisfied their legal and ethical concerns, lawyers at Qwest refused to negotiate any further.

## **Internet Archives<sup>38, 39</sup>**

On November 26, 2007, the FBI served the online library Internet Archive with a national security letter that demanded access to records regarding the usage information of one particular client of the Archive's services. At the same time, the FBI imposed a gag order on the site's founder, Brewster Kahle, which prevented him from in any way discussing the information demanded. Internet Archive did not comply, however. Instead, the Archive responded to the NSL by providing the FBI with information that was already available to the public. Meanwhile, Kahle sought the help of the

Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU), who brought suit in December 2007 to challenge the constitutionality of the FBI's use of the NSL, as well as the use of the gag order. As a direct result of this lawsuit, the FBI agreed in April 2008 to rescind the NSL and allow the case to be unsealed, which effectively broke the gag order. Nevertheless, Kahle is still forbidden to discuss the specific information originally demanded.

Internet Archive's resistance is quite unique in that their lawsuit represents one of only a few instances in which court cases have arisen challenging the FBI's use of national security letters. Nevertheless, their success should signal to other businesses that it is possible to resist a NSL.

## **Lessons Learned**

These stories describe business leaders from a variety of different industries who demonstrated tremendous courage in resisting the unlawful demands of government agencies such as the FBI and NSA. Their stories should not only inspire but also inform by serving as models for other business leaders willing to stand up for their customers' right to privacy. As a business leader, there are a few lessons that you should learn from these stories.

### **Consult a Lawyer**

If you ever receive a demand for information that you believe to be unconstitutional from a government agency, you should seek a lawyer before complying with the demand. As a business leader, you should explore and make yourself aware of the different options available for challenging the government's demands. One method is to contact one of the many civil liberties organizations that provide free legal advice, such as the Electronic Frontier Foundation or the American Civil Liberties Union. These organizations will provide you with expert advice in a discreet manner that does not put you or your business in jeopardy. Further, these organizations may even offer to take up and spearhead your case.

### **Do Not Submit Voluntarily to Demands**

In the event that you receive an unconstitutional demand for information, it is imperative that you do not comply. Although the government agency that approaches your business may attempt to coerce you into submitting voluntarily to their demands, you should always be aware that if the demand were legal and involved an urgent matter of national security, that agency would have secured a warrant.

To illustrate this point, consider the stories discussed previously involving Qwest Communications and Las Vegas casinos. In both situations, the intelligence agencies involved refused to submit their demands for information to judicial review. It is clear that these agencies refused to do so because their demands were not constitutional and did not involve urgent national security concerns that would justify overriding basic constitutional protections.

By resisting the demands made of your business, you will force the government agency involved to pass through the appropriate and necessary legal hurdles that are built into our system to prevent abuse. If the agency does obtain a warrant, you will then be able to provide the information demanded secure in the knowledge that you did your utmost to protect your customers' privacy.

Further, although it may seem, in the short term, to be in your business's best interests to comply with an illegal request for information, there may be serious long-term consequences you may not have considered. In addition to potential litigation, if Congress moves to investigate illegal surveillance by national security agencies, it is possible your company's executives could be called before Congress to testify about their actions, which could damage your business's brand and reputation and undermine customers' trust in you.

### **Challenge the Demand in Court**

If you or your business receives an unlawful demand for information, you should strive to challenge that demand in court. The lawsuit that you raise may very well establish the legal framework that makes it possible for other business leaders

to challenge the demands that they receive. Thus, in challenging the government's demand for information, you will not only protect the constitutional rights of your customers, but you will also make it possible for other businesses to protect the rights of theirs. To illustrate this point, consider the above story involving Library Connection. If George Christian, the executive director of Library Connection, had not learned that an internet service provider in New York had successfully challenged compliance with a national security letter, he might not have challenged the NSL that he received.

## Notify Your Customers If Possible

In the event that you receive an unconstitutional demand for information, you should notify the customer or customers whose information the government seeks. In doing so, you enable your customers to challenge the government's demand for their information. It is important to note, however, that there are a variety of situations in which disclosing the existence of the government's demand for information might put your company at risk. In this type of situation, such disclosure is clearly inadvisable.

## Raise Your Concerns

If possible, you should raise, in public, your concerns regarding the government's demand for information. Raising your concerns in public may help to stimulate an open debate that could lead Congress to enact legislation against the intelligence community's unlawful demands. However, if you are unable to do so, you might consider writing an anonymous letter to a major publication such as the *New York Times*, *Washington Post*, or *USA Today* in which you explain your situation and voice your concerns. If you write this letter carefully, you can expose government abuse without putting yourself or your business at risk. Alternatively, consider discussing your concerns with a civil liberties organization (such as the Electronic Frontier Foundation) that can then take action independently.

## Civil Liberties Organizations That Provide Legal Advice

- Electronic Frontier Foundation (<http://www.eff.org/about/contact>)
- Center for Constitutional Rights (<http://ccrjustice.org/contact>)
- American Civil Liberties Union (<http://www.aclu.org/affiliates>)
- Center for Democracy & Technology (<http://www.cdt.org/aboutcontact.php>)

---

### Notes:

1. Robyn E. Blumner. "With Patriot Act, Companies Forced to Play Informant on Customers." *St. Petersburg Times*. 18 May 2003. 8 Aug. 2008. <[http://www.sptimes.com/2003/05/18/Columns/With\\_Patriot\\_Act\\_com.shtml](http://www.sptimes.com/2003/05/18/Columns/With_Patriot_Act_com.shtml)>.
2. "EFF's Class-Action Lawsuit Against AT&T for Collaboration with Illegal Domestic Spying Program." *Electronic Frontier Foundation*. 8 Aug. 2008. <<http://w2.eff.org/legal/cases/att/>>.
3. Michael Sniffen. "Major Business Groups Split With Bush Administration Over Patriot Act." *Associated Press*. 6 Oct. 2005. *CommonDreams.org News Center*. 31 Jul. 2008. <<http://www.commondreams.org/headlines05/1006-06.htm>>.
4. John J. Berlau. "Show Us Your Money: The USA PATRIOT Act lets the feds spy on your finances." *Reason*. Nov. 2003. 31 Jul. 2008. <[http://findarticles.com/p/articles/mi\\_m1568/is\\_6\\_35/ai\\_109085440](http://findarticles.com/p/articles/mi_m1568/is_6_35/ai_109085440)>.
5. "Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power." *Center for Democracy and Technology*. 24 Sep. 2003. 31 Jul. 2008. <<http://www.cdt.org/security/usapatriot/030924cdt.shtml>>.
6. Charles Doyle. "The Patriot Act: A Sketch." Congressional Research Service. 18 Apr. 2002. 11 Aug. 2008. <<http://www.fas.org/irp/crs/RS21203.pdf>>.
7. Charles Doyle. "The Patriot Act: A Sketch." Congressional Research Service. 18 Apr. 2002. 11 Aug. 2008. <<http://www.fas.org/irp/crs/RS21203.pdf>>.
8. Eunice Moscoso. "Demand for Data by Feds on the Rise." *Cox Washington Bureau*. 7 Aug. 2003. 11 Aug. 2008. <<http://www.federalobserver.com/print.php?aid=6378>>.
9. USA PATRIOT Act, Section 311.
10. "Let the Sun Set on PATRIOT – Section 215." *Electronic Frontier Foundation*. 11 Aug. 2008. <<http://w2.eff.org/patriot/sunset/215.php>>.
11. "The Patriot Act: Where It Stands." *American Civil Liberties Union*. 11 Aug. 2008. <<http://action.aclu.org/reformthepatriotact/whereitstands.html>>.
12. "ACLU Says Justice Dept.'s PATRIOT Act Website Creates New Myths About Controversial Law." *American Civil Liberties Union*. 26 Aug. 2003. 31 Jul. 2008. <<http://www.aclu.org/safefree/patriot/1676oprs20030826.html>>.

13. "Analysis of the USA Patriot Act Related to Libraries." *American Library Association*. 11 Aug. 2008. <<http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis.cfm>>.
14. "The USA PATRIOT Act." *American Library Association*. 11 Aug. 2008. <<http://www.ala.org/ala/washoff/woissues/civilliberties/theusapatriotact/usapatriotact.cfm>>.
15. John Solomon. "FBI Finds It Frequently Overstepped in Collecting Data." *Washington Post*. 14 Jun. 2007. 11 Aug. 2008. <<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453.html>>.
16. Burke Hansen. "Secretive FBI 'National Security Letters' to ISPs, Telcos Halted." *The Register*. 10 Sep. 2007. 11 Aug. 2008. <[http://www.theregister.co.uk/2007/09/10/nsl\\_fbi\\_decision/](http://www.theregister.co.uk/2007/09/10/nsl_fbi_decision/)>.
17. "National Security Letters." *Electronic Privacy Information Center*. 18 Mar. 2008. 11 Aug. 2008. <<http://epic.org/privacy/nsl/default.html>>.
18. "The Patriot Act: Where It Stands." *American Civil Liberties Union*. 11 Aug. 2008. <<http://action.aclu.org/reformthepatriotact/whereitstands.html>>.
19. "A Review of the Federal Bureau of Investigation's Use of National Security Letters." *U.S. Department of Justice, Office of the Inspector General*. Mar. 2007. 11 Aug. 2008. <<http://www.usdoj.gov/oig/special/s0703b/final.pdf>>.
20. Burke Hansen. "Secretive FBI 'National Security Letters' to ISPs, Telcos Halted." *The Register*. 10 Sep. 2007. 11 Aug. 2008. <[http://www.theregister.co.uk/2007/09/10/nsl\\_fbi\\_decision/](http://www.theregister.co.uk/2007/09/10/nsl_fbi_decision/)>.
21. "How the USA PATRIOT Act Redefines 'Domestic Terrorism.'" *American Civil Liberties Union*. 6 Dec. 2002. 11 Aug. 2008. <<http://www.aclu.org/natsec/emergpowers/14444leg20021206.html>>.
22. "Executive Order 13224 (Fact Sheet)." *U.S. Department of State*. 20 Dec. 2002. 11 Aug. 2008. <<http://www.state.gov/s/ct/rls/fs/2002/16181.htm>>.
23. "How the USA PATRIOT Act Redefines 'Domestic Terrorism.'" *American Civil Liberties Union*. 6 Dec. 2002. 11 Aug. 2008. <<http://www.aclu.org/natsec/emergpowers/14444leg20021206.html>>.
24. "Executive Order 13224 (Fact Sheet)." *U.S. Department of State*. 20 Dec. 2002. 11 Aug. 2008. <<http://www.state.gov/s/ct/rls/fs/2002/16181.htm>>.
25. Thomas Frank. "Homeland Security rules on data collection rile businesses." *USA Today*. Jan. 2008. 9 Jan. 2008. <[http://www.usatoday.com/tech/news/techpolicy/2009-01-06-security\\_N.htm](http://www.usatoday.com/tech/news/techpolicy/2009-01-06-security_N.htm)>.
26. John J. Berlau. "Show Us Your Money: The USA PATRIOT Act lets the feds spy on your finances." *Reason*. Nov. 2003. 31 Jul. 2008. <[http://findarticles.com/p/articles/mi\\_m1568/is\\_6\\_35/ai\\_109085440](http://findarticles.com/p/articles/mi_m1568/is_6_35/ai_109085440)>.
27. John J. Berlau. "Show Us Your Money: The USA PATRIOT Act lets the feds spy on your finances." *Reason*. Nov. 2003. 31 Jul. 2008. <[http://findarticles.com/p/articles/mi\\_m1568/is\\_6\\_35/ai\\_109085440](http://findarticles.com/p/articles/mi_m1568/is_6_35/ai_109085440)>.
28. John J. Berlau. "Show Us Your Money: The USA PATRIOT Act lets the feds spy on your finances." *Reason*. Nov. 2003. 31 Jul. 2008. <[http://findarticles.com/p/articles/mi\\_m1568/is\\_6\\_35/ai\\_109085440](http://findarticles.com/p/articles/mi_m1568/is_6_35/ai_109085440)>.
29. "National Security Letters." *Electronic Privacy Information Center*. 18 Mar. 2008. 11 Aug. 2008. <<http://epic.org/privacy/nsl/default.html>>.
30. "SCUBA Associations Give Records to FBI without Telling Members; EFF's Legal Director Responds." *Electronic Frontier Foundation*. 12 Jul. 2002, 31 Jul. 2008. <<http://www.eff.org/effector/HTML/effect15.19.html#III>>.
31. Barton Gellman. "The FBI's Secret Scrutiny." *Washington Post*. 6 Nov. 2005, 31 Jul. 2008. <[http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366_pf.html)>.
32. "ACLU: Gagged National Security Letter Recipient Condemns Excessive Secrecy as Government Appeals His Case." *Common Dreams Progressive Newswire*. 5 Nov. 2007. 31 Jul. 2008. <<http://www.commondreams.org/cgi-bin/newsprint.cgi?file=/news2007/1105-03.htm>>.
33. "My National Security Letter Gag Order." *Washington Post*. 23 March 2007. 31 Jul. 2008. <<http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html>>.
34. Peter Pollack. "Patriot Act Smackdown: Librarians 1, FBI 0." *arstechnica.com*. 27 Jun. 2006. 31 Jul. 2008. <<http://arstechnica.com/news.ars/post/20060627-7150.html>>.
35. Barton Gellman. "The FBI's Secret Scrutiny." *Washington Post*. 6 Nov., 2005. <[http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366_pf.html)>.
36. Leslie Cauley. "NSA Has Massive Database of Americans' Phone Calls." *Washington Post*. 11 May 2006. 31 Jul. 2008. <[http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm)>.
37. Tom Zeller. "Quest Goes From the Goat to the Hero." *New York Times*. 15 May 2006. 31 Jul. 2008. <<http://www.nytimes.com/2006/05/15/technology/15link.html?ex=1305345600&en=bc97d6acbf0429f7&ei=5090&partner=rssuserland&emc=rss>>.
38. Ellen Nakashima. "FBI Backs Off From Secret Order for Data After Lawsuit." *Washington Post*. 8 May 2008. 31 Jul. 2008. <<http://www.washingtonpost.com/wp-dyn/content/article/2008/05/07/AR2008050703808.html>>.
39. Grant Gross. "Internet Archive Challenges F.B.I.'s Secret Records Demand." *New York Times*. 7 May 2008. 31 Jul. 2008. <[http://www.nytimes.com/idg/IDG\\_852573C40069388000257442004ECECE.html?ref=technology](http://www.nytimes.com/idg/IDG_852573C40069388000257442004ECECE.html?ref=technology)>.