

CANADIAN CORPORATE COUNSEL ASSOCIATION

SPRING CONFERENCE 2005
TORONTO, ONTARIO

USA PATRIOT ACT:
THE INTERSECTION OF PRIVACY AND TERRORISM

Daniel C. Oliverio, Esq.
Kevin M. Kearney, Esq.
Hodgson Russ, LLP
One M&T PLaza, Suite 2000
Buffalo, New York 14203
Phone: (716) 856-4000
Fax: (716) 849-0349

I. Introduction

The passage of the USA Patriot Act (“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”) shortly after the tragedy of September 11, 2001 represents one of the most comprehensive limitations of individual privacy rights, whether statutory or judicial, in the history of the United States. The stated purpose of the Act is to enable law enforcement officials to identify, track and prosecute those responsible for terrorist attacks like those of September 11. The Act, passed by Congress on October 26, 2001, within six weeks of the September 11 attacks, amends 15 existing statutes and adds a number of new provisions. It provides federal law enforcement with a host of enhanced powers, especially in the areas of surveillance, information-gathering, and allows the law enforcement and counter-intelligence arms of the United States government to share information. It also reinforces existing federal money-laundering provisions and places substantial new responsibilities on banks and financial institutions to identify and report suspicious banking and financial activities. Its immigration provisions restrict entry into the United States of non-citizens and those suspected of being terrorists and expedites the process for expelling suspected terrorists already in the United States. The Act substantially redefines and broadens the definition of what is a federal terrorism crime and increases the penalties for terrorism-related offenses. Procedurally, the Act also extends the statute of limitations for terrorism-related offenses, thereby acknowledging the complex and often time-consuming investigative hurdles required to marshal evidence sufficient to sustain successful prosecutions.

So dramatic and encompassing are many of the amendments, especially those addressing wire-tapping and foreign counter-intelligence gathering, that Congress provided for

the “sunset” of many of those provisions on December 31, 2005. Nonetheless, the debate over the efficacy and scope of the Act continues. And the debate will no doubt intensify as Congress considers the “sunset” provisions and very likely substantial additional amendments to the Act proffered by federal law enforcement officials and the Bush administration.

This article will focus on some of the surveillance provisions of the Act and how they have impacted the Supreme Court’s prior interpretations of the United States Constitution’s fourth amendment prohibition against unreasonable searches and seizures.

II. The Surveillance Provisions of the Patriot Act and the Fourth Amendment of the United States Constitution

The fourth amendment of the United States Constitution provides as follows:

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 in particularly describing the place to be searched and the persons or things to be seized. *United States Constitution Amendment IV*

The Supreme Court of the United States has interpreted the fourth amendment’s prohibition against unreasonable searches and seizures to extend to private conversations in addition to the more traditional notions of private property and privacy of the person. The Government may not eavesdrop or overhear what are generally accepted to be “private conversations” (i.e., where

there is an expectation of privacy) under the fourth amendment. Accordingly, the fourth amendment, in the first instance, protects citizens of the United States or those lawfully within its borders from intrusions upon property, both real and personal and, as well, the interception of private conversations and communications, without a warrant requiring an evidentiary showing of probable cause that such intrusion will lead to evidence of a crime.

Gathering of evidence in violation of the fourth amendment precludes law enforcement from using such unlawfully obtained evidence in a later proceeding. An accused is typically afforded the opportunity to fully test evidence obtained under the warrant requirements of the fourth amendment to ensure the regularity of the process and the Government's compliance with the law.

Over the years, Congress has responded to interpretations of the fourth amendment advanced by the Supreme Court by enacting legislation that, while abiding the dictates of the Constitution, enables law enforcement to capture otherwise private communications or conduct searches. For example, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 generally prohibits electronic eavesdropping on telephone conversations, face-to-face conversations or computer and other forms of electronic communications upon the ground that such eavesdropping would violate the fourth amendment. Under Title III, however, law enforcement authorities are afforded a narrowly defined exception for electronic surveillance (i.e., electronic eavesdropping) to be used as a last resort in the investigation of specifically enumerated serious crimes. An application for a warrant under Title III requires approval by a senior justice department official; rigorous evidence of probable cause; must specify with particularity the duration and scope of the surveillance; must specify the

conversations that may be seized; and must specify the efforts that must be taken to minimize the seizure of innocent conversations. Title III also provides that parties to any of the seized conversations must be notified after the Title III eavesdropping order expires. Importantly, Title III eavesdropping wiretaps may only be used in the investigation of statutorily specifically enumerated crimes and under careful supervision of the court.

The courts and Congress have carved out further exceptions from the fourth amendment and Title III by permitting law enforcement to obtain pursuant to a warrant or court order telephone records, email held in third party storage, and similar electronic information in connection with any criminal investigation (unlike Title III's specific crimes provision) and without any extraordinary levels of approval through the Department of Justice. While these provisions still require application to a court and a showing of probable cause, like any other search warrant, the particularity and minimization provisions of Title III, as well as the limited crimes exception, are not required.

The courts and Congress have traditionally recognized yet another exception to the fourth amendment by permitting the Government to apply for a court order for the installation of what is commonly referred to as a "trap and trace" device which acts as a type of secret caller identification. These devices, commonly referred to as "pen registers," are obtained by a mere certification by the Government to a court that use of the device is likely to produce information relevant to an ongoing investigation of any crime. Pen registers record the identity of the numbers assigned to the telephone lines activated by a particular communication; i.e., they provide a record of the numbers involved in a particular telephone call. Trace and trap/pen

register certifications and orders need not ever be revealed to the participants unlike a wire-tap or search warrant.

The Patriot Act significantly amends and enhances (at least according to some commentators) the ability of the Government to work within the scope of the fourth amendment prohibition against unreasonable searches and seizures with respect to both tangible evidence and surveillance evidence. The Patriot Act enhances the Government's surveillance powers in four primary areas:

- ▲ Under §215 of the Act, it expands the Government's ability to examine records of individual activity in the custody of third-parties.
- ▲ In §213, it expands the Government's ability to obtain warrants to search private property without notice to the owner of that property (i.e., "sneak and peak" searches).
- ▲ In §218, it expands what was previously a very narrow provision of the Foreign Intelligence Surveillance Act allowing the collection of "foreign intelligence information" without any warrant.
- ▲ In §214, it expands the power of the Government to use "trap and trace" searches to obtain electronic "addressing" information identifying the origin and destination of computer communications, if not content.

Section 215 of the Act

Section 215 of the Act makes it easier for law enforcement authorities to gain access to personal records held by a third-party for what is alleged to be counter-terrorism related purposes. And the records covered by this section include those held by any third party including, for example, physicians, libraries, book stores, internet service providers, accountants, retail stores and practically every other third-party who may have on-hand either electronic or other records of a particular person's activities with that party. Under §215, the Government no longer needs to show that the subjects of these types of orders are "agents of a foreign power" as before or that there is a "reasonable suspicion" that the records requested are related to criminal activity (much less that there is "probable cause" to believe they are related to criminal activity under the fourth amendment). Instead, a Government agent must only certify that the request is related to an on-going "terrorism or foreign intelligence investigation" without need for any documentary or other evidentiary proof thereof. If so, the Court must then grant the order for the turnover of the requested records.

While §215 specifically states that the request and investigation must not be based solely upon activities protected by the first amendment to the Constitution of the United States, the documents or information requested may certainly have first amendment implications; for example, the order may demand turnover of a list of books that a person may have read, the websites they may have visited, or correspondence they may have authored to another.

Importantly, since the person or entity to whom the turnover order is directed may not disclose the request to anyone, it is possible that the ultimate subject of the request (i.e., the

party to whom the request relates) may never find out that their personal records were examined by the Government in connection with an investigation allegedly relating to terrorism or clandestine intelligence activities. In short, unlike a fourth amendment search warrant, there are no checks and balances or ability to “test” the search against the fourth amendment standard.

Interestingly, §215 expressly provides that production of records under such an order does not act as a waiver of any privilege in any pending or future proceeding. One question that remains unanswered is whether the Government can obtain information covered by the attorney-client privilege under §215.

Much of the controversy over §215 centers around the lack of notice and any requirement that the Government show “probable cause” as is required under the fourth amendment before obtaining the requested information. There is concern that the mere certification provisions of §215 and the inability to “test” compliance will lead to Government abuse and overreaching. While the Attorney General is required to report to Congress semi-annually about the number and type of applications made under §215, the statute does not provide for any other oversight or review of such applications for abuse, misuse, or non-compliance.

Section 213 of the Act

Section 213 of the Act provides the Government with “sneak and peak” powers to conduct secret searches of property without any notice or at best delayed notice to the owner.

As discussed above, the fourth amendment of the Constitution typically requires a search warrant before law enforcement may enter upon a person's premises to search for and seize evidence of a crime. Obtaining a search warrant requires an application to the court setting forth in evidentiary form facts sufficient to support the conclusion that there is "probable cause" to believe that evidence of a crime can be found in a specific and particularized location such as a house, apartment or other property. That search warrant application must be accompanied by sworn affidavits and offers of proof in evidentiary form before it can be granted by a court. Search warrants also provide a detailed description of the premises to be searched and what specifically law enforcement is permitted to search for on the premises within a defined time period. Moreover, the fourth amendment has been construed to require, in most instances, a "knock and announce" requirement and notice to the owner or party controlling the premises of the search. Typically, a copy of a search warrant is presented to the owner or party controlling a particular location as is an "inventory" of the items seized or taken pursuant to the warrant.

Under §213 of the Act, a court may now issue a warrant to search property for evidence of a criminal offense and delay notice of such search if the court finds reasonable cause to believe that providing immediate notice of the execution of the warrant may have an "adverse result" on the investigation and provided the warrant prohibits the actual seizure of any tangible property. Later notice within a "reasonable period" after the warrant's execution is required, but that period may be extended by the court for good cause shown. In short, §213 of the Act enables law enforcement to obtain a search warrant providing for a secret search of property, and an inspection of that property or anything that is in it, related to the investigation of any crime (not just crimes of terrorism). This section has been roundly criticized because of its

modification of long-standing “knock and announce” requirements under the fourth amendment and what appears to be the limitless power of the Government, unsupervised, to conduct a “sneak and peak” search of property without simultaneously informing its owner.

Section 218 of the Act

The Foreign Intelligence Surveillance Act was passed in 1978 and created an exception to the fourth amendment’s requirement of probable cause to search when the purpose of a warrant or a wire-tap was to gather “foreign counter-intelligence information” as opposed to evidence of a crime. Under FISA, a secret court, convened expressly for hearing applications for FISA warrants, determined whether the Government could avoid the fourth amendment while obtaining permission to wire-tap or conduct a search for foreign counter-intelligence purposes. Under FISA before the amendments of the Act, it was only necessary for the Government to certify that “the purpose” of a surveillance request or warrant to search was to obtain foreign counter-intelligence information. Commentators have often questioned whether the Government has attempted to use FISA surveillance orders to avoid the exacting requirements of a Title III wire-tap order of the less-exacting, but substantial probable cause requirements, of a search warrant.

Under §218, FISA warrants may now be granted where counter-intelligence is certified to be “a significant purpose” rather than “the purpose” of an application for a warrantless wire-tap or search. Moreover, the Act now permits sharing of criminal and foreign counter-intelligence information among law enforcement and the U.S. intelligence community.

Accordingly, all of the provisions of FISA enabling the Government to obtain information regarding foreign counter intelligence in the United States without the scope of the strict requirements of the fourth amendment have now been broadened to cases where foreign counter-intelligence is merely “a significant purpose” of the investigation, but not the sole purpose. Warrantless wire-taps, pen registers for emails, and access to any other types of tangible items, etc. gathered under FISA are now available to law enforcement personnel in appropriate cases and in expanded circumstances. Section 218 of the Act blurs the distinction between what was previously separate investigative purposes (i.e., investigations of crimes and gathering of foreign counter-intelligence information) in an effort to provide a unified defense against terrorism. By blurring the line, critics have contended that the Government now has the ability to circumvent the protections of the fourth amendment by merely certifying that a particular request to wire-tap or search has as its “significant purpose,” the gathering of foreign counter-intelligence information and then sharing such information as part of a criminal case.

Section 214 of the Act

Section 214 of the Act amends the Government’s pen register and trap and trace authority under FISA. As described above, pen registers and trap and trace searches are the least intrusive of the types of searches permitted under the fourth amendment. They require that the Government merely certify to a court that the issuance of such a warrant would be “relevant” to an ongoing criminal investigation. There is no separate “probable cause” or standard as is required for a search warrant under traditional fourth amendment criteria or the enhanced criteria of a Title III wire-tap. A typical pen register or trap and trace search is also limited to identifying

information such as, for example, the telephone numbers comprising each end of a telephone conversation.

Under the amendments provided by §214 of the Act, pen register and trap and trace orders issued by a court are no longer only valid in that court's jurisdiction, but can be made valid anywhere in the United States. These "roving" warrants, commentators contend, remove any control from the court and place discretion in the hands of law enforcement who is then able to direct the warrants to particular places either unknown or undisclosed to the court in the original application.

Section 214 of the Act also addresses the use of pen registers or trap and trace warrants to capture internet communications in a way that critics contend weakens the standards for access to transactional or content-oriented data. For example, the Government interprets the "header" portion of an email message to be transactional information available through a warrant issued under the minimal requirements of trap and trace or pen register applications. Critics contend that the header of an email may also include the subject line which is part of the substance of the communication in many cases and therefore should be subject to the traditional fourth amendment warrant or Title III requirements.

There is also dispute between the Government and bar about whether a list of URLs or website addresses that a person visits is transactional data that is subject to search under the minimal standards of a pen register or trap and trace warrant. The Government has taken the position that website addresses and similar URL information is transactional. The courts have yet to finally decide those issues under §214.

Miscellaneous Provisions

Section 218 of the Act permits criminal investigators to retrieve the content of electronic communications in storage (e.g., email) with a search warrant, and if that communication has been in remote storage for more than 180 days, without even notifying the subscriber. The Act also treats voicemail like email; voicemail is subject to the search warrant standard, rather than the more demanding requirements of Title III. And if in what will likely be a rare case the Government is unable to effect its purposes using the expanded powers of the Act to obtain surveillance, the Title III predicate offense list now includes cybercrime and a host of additional terrorism-related crimes. Accordingly, the highly intrusive eavesdropping capabilities of a Title III wire-tap are now readily available in the investigation of terrorism-related crimes and cybercrime if all else fails.

III. Conclusion

The Patriot Act, passed a mere six weeks after the tragedy of September 11th, arguably grants to law enforcement most of its “wish list” of statutory amendments relating to surveillance and information-gathering in the continuing fight against terrorism. Critics contend that the Patriot Act goes too far and that it was passed without sufficient study or investigation of its potential effects upon the fourth amendment and the privacy rights of citizens. And while the “sunset” provisions of the Act will necessarily be hotly debated on or before December 31, 2005, prevailing opinion indicates that Congress will refrain from any significant amendment of the Act’s surveillance provisions in the face of continuing terrorist threats.