Return to Privacy Module V

INTRODUCTION TO MODULE V: THE USA PATRIOT ACT, FOREIGN INTELLIGENCE SURVEILLANCE and CYBERSPACE PRIVACY[1]

I. INTRODUCTION

USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, USAPA), H.R. 3162, was passed on October 26, 2001. The bill is 342 pages long and amends over 15 different statutes. The legislation was written extremely quickly - only five weeks passed between the introduction of the first draft of the act and its final passage into law. As a result of the haste with which the act was passed, the vast majority of the provisions in the act contain sunset provisions under which they will become inactive on December 31, 2005. Despite the sunset provisions, the act has far reaching impact on the privacy rights of U.S. citizens. Many organizations interested in protecting civil liberties are concerned that the act inappropriately encroaches on the privacy rights of American citizens and justly so.

The act was passed as a response to the September 11th terrorist attacks, and provides for broad changes to current law. Some of the changes seem logical and necessary given the circumstances. For example, the act calls for increased government spending on airport security, financial relief for the families of the victims of the September

11th attacks, and provisions ensuring that the charitable contributions made after the attacks are spent properly. USA Patriot contains substantial amendments to many federal statutes.

For example, the Act creates new ways in which the government can monitor individuals and obtain private information. Changes to privacy law include such provisions as increased monitoring of financial transactions, creation for a DNA bank to identify terrorists and other violent offenders, required disclosure to the CIA and FBI of information obtained during grand jury proceedings, changes in the scope of search warrants for electronic information, and greatly increased CIA and FBI powers to monitor individuals. Although the statute gave the government new powers in many arenas, this Introduction will focus on significant changes to current law that affect informational privacy in cyberspace. Specifically, in the following sections we examine how USAPA expands the availability of the four main methods of cybersurveillance: wiretaps, search warrants, pen/trap orders, and subpoenas.

II. BACKGROUND: THE DISTINCTION BETWEEN FOREIGN INTELLIGENCE SURVEILLANCE AND DOMESTIC SURVEILLANCE.

There are currently two different forms of authority that can be invoked in order to justify surveillance - intelligence authority under the Foreign Intelligence Surveillance Act (FISA), and authority to pursue a criminal investigation under a variety of federal statutes. FISA , enacted in 1978, creates authority to conduct searches and surveillance of foreign agents or foreign governments with the goal of gaining intelligence information.

There are several important differences between a FISA intercept order obtained under intelligence authority

and an intercept order obtained under authority to investigate criminal matters. Most importantly:

(1) There is no probable cause requirement for a FISA search;

(2) There is no requirement of notice for a FISA search;

(3) The target of a FISA search cannot obtain discovery of the FISA court order application. As a result, the target of a FISA search cannot effectively challenge a wiretap or search conducted under FISA authority; and

(4) Finally, FISA created a secret court--one comprised of a panel of federal judges whose hearings, decisions, and makeup are all secret. Moreover, once it obtains the intercept order, the government need not report back to the secret Court.

Because of the secrecy of FISA investigations and the latitude that law enforcement agents are given in FISA investigations, the scope of such investigations had traditionally been very narrow. Traditionally, FISA investigations could be used only when foreign intelligence gathering was ***the*** primary purpose. The targets of FISA were agents of foreign lands or their governments.

USAPA significantly broadens the scope of situations where FISA intelligence authority can be invoked. For example, under USAPA, FISA surveillance authority may be used even if the primary purpose is a criminal investigation intelligence gathering need only be ***a*** significant purpose. Thus, FISA can be invoked to conduct a criminal investigation despite an inability to make a showing of probable cause.

Even the limited requirements imposed under the amended FISA disappear if the electronic surveillance is

directed solely at communications used exclusively between foreign powers and when it is unlikely that communications to which a U.S. person is a party will be intercepted. Under the new law, in such cases the government may conduct surveillance for up to a year without a court order.

One fear expressed by many privacy advocates is that FISA might become a back door source of authority for government to conduct domestic surveillance not necessarily involving the threat of terrorism. Residents of countries other than the U.S. are certainly subject to this increased power as well.

III. GOVERNMENT POWER TO CONDUCT CYBERSURVEILLANCE INCREASED

A. Pen Register Or Trap And Trace Orders (USAPA 214, 216)

Currently, law enforcement involved in intelligence investigations can obtain a pen register or trap and trace order (pen/trap order) under which they can have access to numbers dialed and received by a particular phone. In order to obtain a pen/trap order, law enforcement must show that the information that they are seeking to obtain is relevant to an ongoing criminal investigation and that the suspect that they are tracking is in communication with someone involved in international terrorism or intelligence activities. This is a much lower standard than the probable cause standard used in criminal investigations.

USAPA 214 and 216 reduce the standard even further under USAPA 214, the in communication with requirement is deleted. Thus, law enforcement must simply show that the information they are seeking is relevant to an ongoing criminal investigation. Under USAPA 216, when law enforcement requests a

pen/trap order from a judge, the judge *must* issue it. The judge has no discretion to refuse. In other words, though a judge may view the request as unnecessary or even unjust, the judge has no power to refuse to issue the pen/trap order.

Also, USAPA §216 extends the scope of information that can be obtained using a pen/trap order. Traditionally, pen/trap orders could only be used to obtain telephone numbers dialed and received. However, under USAPA §216, law enforcement may now have access to §dialing, routing and signaling§ **information**. The reference to §routing§ information refers specifically to internet use§for either email or browsing. The Patriot Act expressly states that "contents" of communications may not be obtained with trap/trace orders, but USAPA does not define the term.[2]

Thus, one fear is that government agents may, under this extremely low standard, obtain internet routing information that would show what websites a suspect visited and what they did while on those websites. Unlike a telephone call, where the numbers dialed and received can easily be separated from the content of the phone call, this is not currently the case with a packet-switched network like the internet.§ [For an explanation of packet switching, see the introduction in Module I entitled Internet 101:§ An introduction to how the Internet works.]§ Under the low standards for trap/trace orders, because the government is authorized to obtain only the numbers dialed/received, the authorities do not have permission to listen to the content.§ However, content cannot easily be separated from internet routing information.

As a result, in order to obtain an email address, for example, law enforcement must be given access to the entire email packet (which includes content). Law enforcement is then entrusted with viewing only the address and deleting the content without viewing it.

Moreover, with internet browsing, content cannot easily be separated from internet routing information. Suppose someone initiates a Google search looking for information about terroism. Suppose she Googles jihad.com followed by a search for bombs.com, Osama.org, and then ACLU, followed by a hit to each of those websites. At this point, it is no longer possible to separate the routing information from the content of the pages she viewed. The content is revealed by the website routing and webpages URLs that she has obtained.

Civil liberties organizations question giving law enforcement such access to information such as the websites a person visited without substantially higher burden being put upon the government to conduct such a search. Indeed, some of the technologies used to obtain routing information also gather information about other users of the same ISP. For example, Carnivore must be relied upon tol gather information not only about the target and about other customers of that ISP. The FBI is then entrusted with filtering out non-relevant information.[3] This raises serious concern about the privacy rights both of the parties being investigated, and parties who are not subject to the information but are simply customers of the same ISP as the target.

Also, 216 pen/trap orders can be served on any ISP. In effect, a federal judge or magistrate in one jurisdiction can issue a blank pen/trap order that does not name the ISP that is subject to the search. It can thus

be used to search any ISP in the United States. Like the provision allowing search warrants to be executed in any district, this encourages forum shopping on the part of law enforcement, and also limits the ability of the ISP to challenge the pen/trap order. USAPA §216 does not have a sunset provision.

B. Increased Scope Of Subpoenas (USAPA §210)

Under prior law, the government could use a subpoena to compel an ISP or website to release the following information about their subscribers: customer's name, address, length of service, and method of payment (method includes only whether payment was by credit card, direct withdrawal from bank account etc.) The government could *not* get credit card numbers, bank account numbers or other more specific identifying information via a subpoena. Under USAPA § 210, the government may now use a subpoena to obtain credit card numbers and bank account numbers. Law enforcement argues that this is essential information as many people register with websites using false names, thus credit card and bank information is the only way to get a positive identification of a suspect. However, there is no judicial review involved in the subpoena process. As a result, there is no check on law enforcement to ensure that they have proper grounds for their request. Thus, broadening the scope of information that they may request via subpoena raises serious issues about allowing law enforcement to have access to private information without any outside §audit§ of the legitimacy of their requests.

C. § Interception of Voice Communications and Stored Voice Mail (USAPA §§202, 209)

-

Prior to the passage of USAPA, government access to stored email communications was governed by the

Electronic Communications Privacy Act (28 USC §2703) and government access to stored voice mail communications was governed by the federal wiretap statute (18 USC §2510(1)). This difference is due to the distinction between stored electronic data (email) and stored wire communications (voice mail). Under the federal wiretap statue, wiretap orders were required in order to access voice mail that was stored by a third party provider (i.e. voice mail stored by the telephone service provider). But, a search warrant could be used to gain access to and confiscate and answering machine from inside a residence or office. The procedure for obtaining a wiretap order is more complex and time consuming than the procedure for obtaining a search warrant. As a result, law enforcement officers often claimed that their investigations were hampered by the need to obtain the wiretap orders. Also, as technology progressed and MIME (Multipurpose Internet Mail Extensions) technology became more common, problems for this statutory set up arose more frequently.MIME allows emails to contain attachments that may include voice recordings. Thus, to obtain unopened email both a search warrant and wiretap order were required. USAPA §209 changes the way that the wiretap statute and ECPA work. Under USAPA, stored wire communications are governed by the same rules as stored electronic data and both can be obtained with a search warrant (ie. wiretap order not needed). This provision sunsets December 31, 2005.

Also, USAPA §202 adds to the list of crimes for which law enforcement may use wiretaps to investigate. Thus, law enforcement may now obtain a wiretap order for violations of the Compute Fraud and Abuse Act (18 USC §1030). This provision also sunsets December 31, 2005.

IV. § EXPANSION OF POWER OF PRIVATE ACTORS

A. Victims of Hacking May Perform Their Own Investigations (USAPA 217)

-

Section 217 of the Patriot Act allows victims of computer attacks (victims of hacking) acting under the color of law to monitor trespassers on their computer systems. Prior to the passage of USAPA, private individuals were unable to assist law enforcement in investigating and monitoring against attacks by hackers. Now, any private individual who meets the following four requirements may take steps to monitor trespassers on their systems: (1) the owner or operator of the protected computer must authorize the interception of the trespasser s communications (ie. individual users may not take action, rather, the ISP or server owner may take action), (2) the person who intercepts the communication must be lawfully engaged in either a criminal or intelligence investigation, (3) the person acting under color of law must have reasonable grounds to believe that the contents of the communication intercepted will be relevant to the ongoing investigation and (4) investigators may intercept only the communications sent or received by the trespassers. This provision opens the door for system owners to police against those they believe are intruders into their systems. This raises issues about allowable scope of policing - whether system owners may take offensive action to obtain information to catch the hacker, or whether they may simply created defenses for their system. Offensive action could create privacy violations of individuals who have no intent to invade or damage the owners system, and safeguards against this possibility are not explicitly laid out in the statute. This provision sunsets on December 31, 2005.

B. Emergency Disclosures by Internet Service Providers (USAPA 212)

Section 212 of USAPA allows for voluntary disclosure on the part of ISPs of private information including customer records as well as content of electronic transmissions. ISPs are given broad latitude to make such disclosures. The provision states that ISPs may choose to voluntarily disclose private customer information if there is a reasonable belief that it relates to an emergency involving immediate risk of death or serious bodily injury to any person. Thus, ISPs are given authority to disclose private information about their subscribers in order to assist in criminal investigations. However, the provision is for *voluntary* disclosure - ISPs are not required to disclose information unless it is known that it relates to criminal matters. This minimizes the possibility that ISPs will be induced to monitor transmissions for criminal data as there is no incentive to do so.

C. Clarification of Scope of Cable Act

The Cable Act (47 USC 551), which was passed in 1984, set out rigid guidelines under which cable companies could refuse to disclose customer records to law enforcement. For example, under the Cable Act, a cable company did not have to respond to subpoenas or warrants for customer information. Instead, they simply had to notify the customer of the request from law enforcement. The customer was then given a hearing at which the government was forced to justify the request for the records.

Recently, cable companies have expanded from simply providing cable television services to also providing telephone and internet services. As a result, cable companies could refuse pen/trap orders by invoking the Cable Act. Thus, USAPA 211 provides that the trap and trace statutes do apply to disclosures by cable companies with respect to internet and telephone services. Thus, the scope of the Cable Act now applies only to cable television

programming information. There is no sunset provision for this section.

V. OTHER PROVISIONS IMPACTING CYBERSPACE PRIVACY

A. Sneak And Peek Warrants (USAPA 213)

[A sneak and peek warrant is one in which the government obtains a warrant and executes it without providing notice or providing a delayed notice to the target.] The Supreme Court has repeatedly affirmed that the Fourth Amendment protection against unreasonable searches and seizures requires that before a search is performed, law enforcement must obtain a warrant and give notice to the party whose property is subject to the search. There are limited exceptions to this rule. For example, if there is a legitimate fear that giving notice will place a person's life in danger or will cause a suspect to flee, notice can be delayed. Judicial review of the warrant, and the requirement of notice to the party being searched, ensures that the scope of the warrant is limited only to searches necessary for the investigation. It also ensures that the party being searched has an opportunity to assert their Fourth Amendment rights and challenge the scope of an overly broad search warrant. These safeguards help ensure a minimal invasion of privacy.

USAPA 213 creates broad exceptions to the rule that notice must be given in a timely fashion. Under 213, law enforcement must only show that the investigation will be jeopardized by giving notice. Under this low standard, it is easy for law enforcement to conduct searches without giving timely notice to the party being searched. Execution of this sort of sneak and peek search warrant greatly increases the chances that the search will be performed without supervision and will result in an unnecessary invasion of privacy. This section does

not contain a sunset provision.

B. Warrants May Be Executed In Any Jurisdiciton (Usapa 219, 220)

Federal Rules of Criminal Procedure, Rule 49(a) require that a search warrant be obtained within the district in which the search would occur. Some exceptions do exist for extreme situations where it can shown that it is likely that the suspect will flee the district thus requiring a multi-district warrant. USAPA 219, however, provides that search warrants for physical searches relating to investigation of domestic or international terrorism may be issued in any district where any aspect of the terrorism activity occurred, and may be executed within the district of issuance or in any other district. In other words, a single search warrant may apply to searches anywhere in the nation. This is a significant departure from prior law, and does not have a sunset provision.

Similarly USAPA 220 allows for nationwide search warrants for email. As a result, authorities do not have to go to the district where the ISP is located in order to obtain a search warrant, and prosecutors and judges in the districts where the ISPs are located have no control over the process of determining whether a warrant may be obtained.

The justification for this provision is that districts where many ISPs are headquartered (Northern California, for example) have recently been inundated with requests for warrants. However, the argument that it is more efficient to spread the work of issuing warrants seems weak when compared to the resulting infringement on civil liberties. Nationwide email warrants raise serious concerns about the ability of law enforcement to forum shop (i.e. seek a

district where the public or judicial sentiment are favorable to granting warrants) for search warrants. It also makes it difficult for an ISP to challenge the order. For example, if a search warrant was issued by a California court authorizing searches at a small Boston based ISP, it would be extremely difficult for the small ISP to challenge as they would have to retain legal counsel in California. This is both expensive and time consuming for the ISP. Thus, the ISP is less likely to take steps to protect the privacy of their customers, and more likely to simply yield to the search. Similarly, this creates a problem of reasonable notice for the customers of the ISP, and severely upsets the traditional system of checks and balances that exist to ensure that the process is in accordance with constitutional protections.

B. Roving Wiretaps

The Fourth Amendment has been interpreted to require that search warrants specify the location of the search. This ensures that the government cannot engage in random searches (ie. law enforcement cannot use a warrant to search random locations). In the context to warrants for communications, this means that law enforcement officers must specify a certain telephone or internet access point that is the subject of the pen/trap order. Thus, traditionally, roving wiretaps which follow a person rather than a specific phone or internet access point, were not allowed.

In 1986 an exception was made under which law enforcements could obtain a roving wiretap if they could prove to a judge that the suspect was intentionally employing techniques to thwart the effectiveness of a traditional pen/trap order. In order to invoke this exception, law enforcement had to demonstrate that the suspect was purposely switching telephones or internet access points in order to evade a pen/trap order. The judge then could issue a

roving wiretap to follow the suspect from phone to phone. In 1998 the exception was broadened such that law enforcement did not need to show that the suspect had intent to thwart the effectiveness of the wiretap. Thus, if law enforcement alleged that the actions of the suspect had the effect of disturbing the effectiveness of the pen/trap, a roving wiretap can be issued, regardless of the suspect's intent. This is the context in which roving wiretaps were allowed prior to USAPA.

USAPA creates a broad new arena for roving wiretaps. USAPA 206 allows for roving wiretaps to be used in intelligence gathering investigations under FISA. As discussed above, these wiretaps are authorized secretly (by FISA court) and there is no probable cause requirement. And, given that USAPA 216 (discussed above) increases the scope of pen/trap orders to include dialing, routing and signaling information, roving wiretaps are now available to track internet use as well. As a result, law enforcement is empowered to track use of any computer that a suspect may have used. For example, if a suspect that the FBI has a wiretap order for uses a computer in an Internet Cafe in order to access the internet, the FBI has permission under USAPA to track usage of that computer. As a result, the FBI has permission to access information stored on that computer (in the form of cookies etc.) about prior and future users. The other users of that computer have no way of knowing that the FBI is tracking usage of that machine, and thus receive no notice that their private information is being monitored by law enforcement.

VI. MISCELLANEOUS PROVISIONS INCREASING SCOPE and ABILITY OF GOVERNMENT TO GAIN

ACCESS TO PRIVATE INFORMATION

-

A. Broader Definitions of Terrorist Activities

USAPA 802 creates a definition for the crime of domestic terrorism. It is an extremely broad definition under which any crime that appears to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, affect the conduct of a government now falls under the heading of domestic terrorism. Thus, given the broad scope of the offense, broad latitude is created for investigation of possible terrorism activities, making it easier for government investigators to obtain private information in pursuit of such an investigation. Similarly, USAPA 808 adds to the list of offenses that comprise the federal crime of terrorism. Of interest is the addition of new computer crimes to the list. Again, this increases the scope of permissible government investigations.

B. Reduced Protections in Criminal Procedure

USAPA 809 removes the statute of limitations for certain terrorist offenses, and raises the statute of limitations from five years to eight years for others. The application of this change is retroactive, meaning that the increased statute of limitations applies to crimes that occurred before the passage of the bill. Thus, an incentive is created to pursue investigations and seek private information relating to individuals suspected of planning terrorist activity many years in the past. This increases the number of individuals whose private information will be subject to investigation.

USAPA §812 permits tracking and oversight of convicted terrorists even after their release from prison. Under this provision, certain individuals will be subject to lifelong tracking and supervision.

C. Increased Power of CIA

USAPA greatly increases CIA access to information about private citizens. USAPA provides for several instances where information gathered may be shared with the CIA. USAPA §203 permits law enforcement agents to provide the CIA with foreign intelligence information revealed to a grand jury. USAPA §203 also permits law enforcement officers to share information with the CIA when they intercept telephone and internet conversations. A court order is not required for information release under either of these provisions. USAPA §203 also allows the CIA to share this information with foreign governments, regardless to the risk that it may cause to members of s suspect§s family who are living abroad.§

D. Increased Spending for Surveillance

USAPA §816 authorizes spending on computer forensic laboratories. It requires the Attorney General to establish regional computer forensic laboratories and to provide support and training on computer forensic investigative techniques. Such techniques enable the recovery of information that has been deleted from a hard drive as well as techniques for monitoring internet transmissions.

USAPA §103 authorizes spending of over $200 million each year for the next three years on the FBI§s technical support center. The technical support center develops surveillance technologies and maintains several surveillance operations.

[1] This Introduction is based on a substantial research paper prepared by Emily E. Terrell (LLS 04). The bibliographic sources for the Introduction include:

[2] Although the term "content" has been defined in an analogous context, see 18 U.S.C. 2510(8) (the term content "includes any information concerning the substance, purport, or meaning of [the] communication"), the term is vague and has not been tested in the context of Internet communications.

[3] See the FBI's pictorial representation of this process: http://www.fbi.gov/hq/lab/carnivore/carnlrgmap.htm