Tammy Mace
Eric Flora

Patriot Act, Privacy

On October 26, 2001, President Bush signed the USA Patriot Act (USAPA) into law. This new law gave great new powers to both domestic law enforcement and international intelligence agencies and has eliminated the checks and balances that gave courts the opportunity to ensure that these powers were not abused. Most checks and balances were put into place after the misuse of surveillance powers by these agencies.

The bill is 342 pages long and makes changes, to over 15 different statutes. This document provides explanation and some analysis to the sections of the bill relating to online activities and surveillance. Just considering the surveillance and online provisions of the USAPA, it is a large and complex law that had over four different names and several versions in the five weeks between the introduction of its first predecessor and its final passage into law.

While containing some sections that seem appropriate -- providing for victims of the September 11 attacks, increasing translation facilities and increasing forensic cyber crime capabilities -- it seems clear that the vast majority of the sections included have not been carefully studied by Congress, nor was sufficient time taken to debate it or to hear testimony from experts outside of law enforcement in the fields where it makes major changes. This concern is amplified because several of the key procedural processes applicable to any other proposed laws, including inter-agency review, the normal committee and hearing processes and thorough voting, were suspended for this bill.

The draft Domestic Security Enhancement Act of 2003, dubbed the Patriot Act II, was marked "confidential" and leaked on February 7. No legislator has yet stepped forward to sponsor it as legislation. And many members of Congress are unhappy about

how the 120-page proposal came about. Members of the Senate Judiciary Committee say the Justice Department

repeatedly denied it was developing a bill to expand the government's spying authority outlined in the Patriot Act, which was shortly after the September 11, 2001, attacks. That act gave the FBI and Justice Department broad new authority to use wiretaps, electronic eavesdropping, and a number of other information-gathering techniques. (yahoo news pcworld)

Our civil liberties as American have taken a tremendous blow with this law, especially the right to privacy in our online communications and activities. There is no evidence that our previous civil liberties were a barrier to the effective tracking or prosecution of terrorists. The government never proved that previous powers of law enforcement and intelligence agencies to spy on U.S. citizens were insufficient to allow them to investigate and prosecute acts of terrorism. The process leading to the passage of the bill did little to ease the concerns of citizens; they amplified them by the inclusion of so many provisions that, instead of being aimed at terrorism, are aimed at nonviolent, domestic computer crime. Many of the provisions appear aimed at terrorism, but the government made no showing that the reasons they failed to detect the planning of the recent attacks or any other terrorist attacks were the civil liberties compromised with the passage of the USAPA (EFF analysis of USAPA).

With one new definition of terrorism and three expansions of previous terms expanded the scope of surveillance exposing more people to surveillance: Watch what you search for on the internet. The USAPA expands all four traditional tools of surveillance, wiretaps, search warrants, pen/trap orders and subpoenas. Their counterparts

under the Foreign Intelligence Surveillance Act (FISA) that allow spying in the U.S. by foreign intelligence agencies have similarly been expanded. This means the government may now spy on web surfing of innocent Americans and that includes terms entered into search engines by just telling a judge that the spying could lead to information that is "relevant" to an ongoing criminal investigation. The person being spied on does not even have to be the target of the investigation. The application must be granted and the government does not have to report to the court or tell the person being spied on what has been done.

Private matters to discuss better revert back to the good old postal system. Section 209 enables stat law-enforcement personnel to obtain a suspect's stored voicemail with a search warrant through the same legal process to gain access to stored email. Before, officers could acquire unopened voicemail stored with a third-party service provider only by getting a wiretap order. This means that the FBI and CIA can now go from phone to phone, and computer to computer without proving that each is being used by a suspect or a target of an order.

Who told you that? Section 210 adds records of session times and durations, temporarily assigned network addresses, (which will help track terrorists' Internet communications), and a customer's means and source of payment for service (including any credit card or bank account number). Before the USAPA, investigators could use a subpoena to compel a limited class of information like a customer's name, address, length of service and means of payment. This law makes two changes to increase how much information the government can get about a person from their internet service provider or anyone else that may handle or store your online communications. It allows

ISPs to voluntarily hand over all "non-content" information without a court order or subpoena (sec.212). It expands on the records that the government may seek with a subpoena without a court review. That includes records of session times and durations, user's login records, temporarily assigned network (I.P.) addresses, means and source of payments, including credit card or bank account numbers (sec. 210, 211).

Cable companies are now providing internet and telephone services in addition to television programming. Some companies have refused to comply with search warrants or subpoenas for records of their customers' telephone and internet use, citing the Cable Act's restrictions. Section 211 clarifies that when a cable company acts as a telephone company or an internet service provider, it must comply with the same laws that apply to any other telephone company or internet service provider. It also preserves the Cable Act's restrictions on the release of information about subscribers' television viewing habits.

Section 212 clarifies that pen registers and trap and trace devices (they enable officers to track which numbers are dialed by a particular telephone) now may be used to collect the non-content portions of criminals' communications over the internet and other computer networks. Now the government can serve a single wiretap, FISA wiretap or pen/trap order on a person or entity nationwide, rather or not the person or entity is named in the order. They don't even have to show a court that the particular information or communication to be gathered is relevant to a criminal investigation. And in the pen/trap or FISA situations, they do not even have to report where they served the order or what information they received. It does not permit collection of the contents of communications (such as the subject line of an email message), making the pen/trap

authority “technology neutral”. Terrorists’ communications can be traced regardless of which method of communication they use.

Section 217 requires that state officials have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to an ongoing investigation, and permits interception only of the trespasser’s own communications. It also clarifies that the definition of “computer trespasser” does not include an internet service provider’s own legitimate subscribers.

An example of what has been discussed is: Secret warrants were first conceived as a legal weapon to fight Cold War espionage, while putting a legal check on domestic spying in the post-Watergate era. The act creating the secret court passed in 1978. The FBI used the warrants to bug foreign embassies in Washington, D.C., and to keep tabs on suspected spies. The Foreign Intelligence Surveillance Act waived the legal standard in criminal cases of “probable cause”, but the spy court could only dispatch agents and their high-tech listening devices for purposes of counterintelligence. The USA Patriot Act expanded the spy court's power with a provision to say, "a significant purpose" must be intelligence gathering. “Both law enforcement and civil liberties groups interpret the change from "the" to "a" as blurring the line between the counterintelligence and criminal work of the FBI in the fight against terrorism” (yahoo news powers test 6).

The FBI's use of secret warrants mushroomed after Congress passed the Patriot Act in response to the Sept. 11 terrorist attacks. Last October, the FBI arrested 5 suspects in the events on September 11th. The FBI used 36 secret warrants to watch and listen to the suspects. The FBI started watching the Portland suspects a few weeks after Sept. 11, when a sheriff's deputy spotted some of them firing guns for target practice in a gravel

pit. Secret warrants in hand, the FBI, helped by Oregon State Police, the Portland Police Bureau and other agencies, began around-the-clock surveillance by early 2002.

Defense attorneys plan to challenge evidence collected under the warrants issued by the ultra-secret Foreign Intelligence Surveillance court, or “spy court”. The case is farther along than other challenges to the new spying powers under provision of the Patriot Act. David Cole, a law professor at Georgetown University in Washington, D.C., said the case could test the constitutional boundaries of the new snooping authority given the FBI after September 11, 2001. The question, he says, is whether it's "constitutional for the government to tap a suspect's phone in a criminal investigation, without probable cause of criminal activity. It's a very important case."

Works Cited

http://story.news.yahoo.com/news?tmpl=story&u=/ap/20030225/ap_on_go_ca_st_pe/spy_powers_test_6, Tue Feb 25, 9:41 AM ET.

Kyle Stock, (Feb. 24, 2003). Patriot Act Expansion Debated. March 16, 2003, http://story.news.yahoo.com/news?tmpl=story&u=/pcworld/20030225/tc_pcworld/109507

Electronic Frontier Foundation, (10-31-01). EFF Analysis Of The Provisions Of The USA PATRIOT Act. March 16, 003, http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

John Ashcroft, (Oct. 26, 2001). National Association of Countries. March 27, 2003, http://www.csac.counties.org/legislation/anti-terrorism/patriot_act_2001.pdf

Executive Summary: Patriot Act Privacy Perspective

President Bush signed the US Patriot Act (USAPA) into law on October 26, 2001. The USAPA expanded law enforcement's power to search. The use of warrants not requiring judicial review and secret warrants has mushroomed since September 11, 2001. Many of the provisions of the USAPA are unnecessary to investigate and prosecute terrorists. The provisions of the patriot act also infringe on our civil liberties, especially our online communications.

This error is compounded because the USAPA has removed the checks and balances that gave courts the opportunity to make sure the powers of law enforcement agencies are not abused. The majority of the content of the USAPA has not been carefully reviewed; not before or after its passage. The Congress passed a document over 300 pages long in roughly 6 weeks, and many of the provisions of the act effectively prohibit judicial review.

Many of the provisions are aimed at nonviolent, domestic computer crime and not bonafide terrorist acts. With the signing of the USAPA the former probable cause requirment for a search becomes the overly broad "relevant to an investigation." A single wiretap can be used to jump from computer to computer without showing a court that the information to be gathered is relevant to a criminal investigation. An ISP can voluntarily hand over all "non-content" information without a subpoena, and if they refuse law enforcement can get a subpoena without judicial review. Secret warrants were first conceived to fight espionage in foreign embassies, but are now a way of going around the probable cause requirement of the fourth amendment that protects US citizens.