

**Testimony of Jerry Berman
Executive Director
Center for Democracy & Technology**

**before the
Senate Judiciary Committee
Subcommittee on Constitution, Federalism, and Property Rights**

**on
Protecting Constitutional Freedoms in the Face of Terrorism**

October 3, 2001

Thank you for the opportunity to testify at this hearing on the momentous question of improving our nation's defenses against terrorism in a manner consistent with our fundamental Constitutional liberties.

CDT joins the nation in grief and anger over the devastating loss of life resulting from the September 11 terrorist hijackings and attacks against the World Trade Center and the Pentagon. Like many, our relatively small staff had friends and acquaintances killed in those heinous acts. We strongly support the efforts of our government to hold accountable those who direct and support such atrocities.

We know from history, however, that measures hastily undertaken in times of peril – particularly measures that weaken controls on government exercise of coercive or intrusive powers – often infringe civil liberties without enhancing security. For that reason, we harbor serious reservations about several bills currently under discussion in this Subcommittee and elsewhere on Capitol Hill. In particular, we are deeply concerned about the Administration's proposed "Anti-Terrorism Act of 2001" (ATA). A recently-circulated alternate package, the Sensenbrenner-Conyers "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act," removes or changes a very few concerns in ATA, but retains

most of the provisions damaging to civil liberties. The concerns we raise in this testimony, unless otherwise noted, apply equally to both bills.

We are deeply concerned about the impact of these bills on constitutional liberties, most particularly in two areas.

First, the ATA and PATRIOT Act tear down the “wall” between the government’s authority to conduct counter-intelligence surveillance against foreign powers and terrorist groups, and its authority to conduct criminal investigations of Americans. In the post-Watergate era, Congress carefully constrained the government from inappropriately mixing its foreign intelligence and law enforcement capabilities, since such mixing would greatly infringe Americans’ constitutional freedoms. The current bills eviscerate that division. Both would change the “primary purpose” standard that permits exceptional surveillance but only when counter-intelligence is “the” primary purpose of an investigation. Instead, the bills would make these extraordinary powers open to all investigations in which counter-intelligence is “a” (or, in the PATRIOT Act, “a significant”) purpose (Sec. 153). As a result, they would permit law enforcement to use constitutionally suspect surveillance techniques—secret searches, bugs, and wiretapping—against Americans in criminal investigations without the protections that Congress originally intended. Besides damaging the civil liberties of law-abiding Americans who may have their communications subjected to secret interception, the bill raises the possibility that criminal prosecutions pursued in this way could be thrown out on constitutional grounds.

At the same time, the ATA and PATRIOT Act allow data collected in a criminal investigation to be shared widely, without judicial review and regardless of whether those activities serve a law enforcement or counter-intelligence purpose (Sec. 154). This would include the content of Title III wiretaps and evidence presented to grand juries, both of which are traditionally protected under law. Such a revision to the law would permit such troubling activities as the development by the CIA or other intelligence agencies of dossiers for Americans not suspected of any criminal activity.

Second, the ATA and PATRIOT Act broadly expand the government’s ability to conduct electronic surveillance and diminish the rights of Americans online. The most problematic sections in this regard are:

- SECTION 101. PEN REGISTER AND TRAP AND TRACE AUTHORITY. Both ATA and PATRIOT would extend to the Internet the current, extremely permissive authority to collect telephone numbers dialed to or from a specific telephone line. But as drafted for Internet, this proposal would provide the government with much more detailed information about a monitored user. It would include not only e-mail addresses, but also URLs detailing activities such as search queries, books browsed, and online purchases. Those monitored do not need to be under investigation, and judges must issue these orders upon a showing of mere relevance, not probable cause.
- SECTION 106. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS. Both ATA and the PATRIOT Act (Sec. 105) say that anyone accessing a computer “without authorization” has no privacy rights and can be tapped by the government without a court order, if the operator of the computer system agrees. This provision eviscerates current protections for electronic communications. Relatively minor violations of an ISP's terms of service – such as using foul language or downloading a copyrighted MP3 file – would allow an ISP to turn over all of that person’s communications without the government obtaining a judicial warrant.

A range of other provisions further expand the government’s surveillance authority, including:

- SECTION 152. MULTI-POINT WIRETAP AUTHORITY. Authorizes FISA “roving” wiretaps, but more broadly than under current criminal law and without necessary guidelines or restrictions on this authority. Thus, if a surveillance target is suspected of using a library computer, then all communications from that library computer might be monitored. We believe a better solution would be to limit this authority’s extent to those devices under the control of a surveillance target.
- SECTION 155. PEN REGISTER/TRAP AND TRACE CONTROLS. Eliminates the only meaningful statutory control (judicial supervision, and a showing that the target is connected to a foreign power or terrorist organization) that exists on use of pen registers and trap and trace devices in intelligence cases.

- SECTION 154. FOREIGN INTELLIGENCE INFORMATION SHARING. Permits distribution of information gathered in criminal investigations – including grand jury information and Title III wiretaps – to a huge number of government employees not involved in law enforcement, without judicial supervision..
- SECTION 156. BUSINESS RECORDS. Allows access to any business records based only on the demand of an FBI agent for intelligence or terrorism investigations with no judicial review or oversight.
- SECTION 157. MISCELLANEOUS NATIONAL-SECURITY AUTHORITIES. Amends several key privacy laws, allowing much greater access to banking, credit, and other consumer records in counter-intelligence investigations, with no judicial review or any showing that such records are relevant to the investigation of a foreign or terrorist agent.

Mr. Chairman, we commend you and the Subcommittee for holding this hearing, and taking the time to consider the legislative proposals put forth by the Administration. Only through the hearing process can you and the American public understand what is being proposed, how it would change current law, and whether the changes are responsive to any deficiencies that the September 11 attack may have revealed. Just as President Bush and his military advisers are taking their time in planning their response, to ensure that they hit the terrorist targets with a minimum of collateral damage, so it is incumbent upon this Congress to avoid collateral damage to the Constitution.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for more than 50 computer, communications, and public interest organizations, companies and associations working on information privacy and security issues.

Context: Law Enforcement and Intelligence Gathering Authorities

As you well know, the current legal structure of the intelligence community was established after Watergate both to improve intelligence and to ensure that the rights of Americans were not eroded by the vast and sometimes vague intelligence authorities that had previously existed. The legal and oversight system for intelligence sprang not just from a concern about civil liberties, but also from a concern about improving the efficacy of intelligence gathering.

A number of the provisions of the Attorney General's bill would change provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA). As the Subcommittee is well aware, FISA gave the FBI and the CIA extremely broad authority to investigate terrorism and to conduct counter-intelligence not only against foreign nationals here in the U.S., but also against American citizens suspected of involvement with terrorist groups. Unlike criminal law, where high standards of government conduct vigorously protect constitutional rights, FISA makes a special exemption for the intelligence community, permitting it to place wiretaps, install bugs, and conduct secret searches without showing probable cause of criminal conduct, giving notice, or even turning the results of the surveillance over to a court for later review. Through FISA, our intelligence community has authority to investigate a sweeping array of individuals and organizations, and through such investigations to defend against acts of terrorism.

Congress designed the FISA statute to be effective, but it recognized that such broad investigative powers, if misapplied, could threaten Americans' constitutional rights. Congress therefore demanded that the powers bestowed by FISA be strongly contained, and that a clear separation – a wall – be erected between the unique and broad standards for surveillance described in FISA, and those used in the rest of the criminal justice system. In particular, Congress wanted to ensure that surveillance under FISA would not be initiated for the purpose of criminal investigations, since such would circumvent the careful protections built into the criminal system. Rules were installed that carefully constrained FISA's usage, and the "wall" precluded information collected through FISA investigations from being used in criminal ones except in cases where the surveillance was initiated and maintained for broader foreign intelligence purposes.

Comments on Administration Proposals

The ATA and the PATRIOT Act would expand already-broad federal government authorities to conduct electronic surveillance and otherwise collect information not only on foreign nationals but on American citizens, while sidestepping constitutional protections. As described above, the bills do not adequately control that expansion, and as a result they damage civil liberties in two ways.

Both bills would change the “primary purpose” standard that permits FISA’s exceptional standards to be used only when counter-intelligence is “the” primary purpose of an investigation. Instead, the ATA and PATRIOT Act propose to open FISA to all investigations in which counter-intelligence is “a” (or, in the PATRIOT Act, “a significant”) purpose (Sec. 153). Such a change clearly threatens the “wall” Congress erected between the government’s normal police authority and its special counter-intelligence powers, with the end result of substantially reducing American’s constitutional protections before the government. The ATA and PATRIOT Act would thus permit law enforcement to use constitutionally suspect surveillance techniques— secret searches, bugs, and wiretapping—against Americans in criminal investigations without the protections that Congress originally intended. Besides damaging the civil liberties of law-abiding Americans who may have their communications subjected to secret interception, the bill raises the possibility that criminal prosecutions pursued using FISA could be thrown out on constitutional grounds.

At the same time, the ATA and PATRIOT Act allow data collected in a criminal investigation to be shared widely and used for any number of activities, without judicial review and regardless of whether those activities serve a law enforcement or counter-intelligence purpose (Sec. 154). Information that could be shared would include the content of Title III wiretaps and evidence presented to grand juries, both of which are traditionally protected under law. Certainly, the government’s law enforcement and intelligence communities should be encouraged to work together, but the terms of their cooperation should be carefully defined, with standards that serve the dual purposes of national security and civil liberties.

Such a lack of controls on the government’s ability to share and distribute information about American citizens – no matter the purpose for which it was collected –

leads to a situation in which entire communities (such as the American Islamic community) might have a surveillance net cast over them by the government's counter-intelligence arm. It leads to the possibility that American citizens disagreeing with the policies of a sitting Administration would have their activities monitored and logged, and dossiers created for them at the CIA or FBI. And it creates the risk that, in our desire for a nation as secure in the future as it has been in the past, we might sacrifice the elements of freedom that made this country as strong as it is.

Even as the ATA and PATRIOT Act alter the division between FISA and the government's normal police powers, they also include numerous, complex provisions extending the surveillance laws, particularly regarding the Internet, even as both bills raise many questions about how such provisions will be implemented. Many of the changes are not related to security concerns raised by the September 11 terrorist attacks. Many are not limited to terrorism cases, but relate to criminal investigations. Some have been proposed by the Justice Department before, and some have been rejected by Congressional committees before, based on their breadth and their impact on liberty.

The proposed language includes sweeping revisions such as a modification of the pen register standard that would allow the government to intercept the content of some Internet communications without any fourth amendment protection (Sec. 101) and a new authority for Internet Service Providers (ISPs) to authorize government surveillance of their users' Internet connections (Sec. 106 in ATA, Sec. 105 in PATRIOT Act). Other changes include the so-called "roving wiretap" authority (Sec. 152), which would permit the government to intercept, for example, *all* Internet communications coming from a public Internet terminal (no matter who is using it) if a suspected terrorist is seen using that terminal.

As technology develops, so too should the government's ability to carry out its law enforcement and counter-terrorism functions. But injudicious changes such as those proposed in the ATA and the PATRIOT Act threaten basic freedoms guaranteed by the constitution. We therefore urge this Subcommittee and the law enforcement and intelligence communities to take a more limited, surgical approach to expanding government powers, both online and off.

A more detailed analysis of the Administration's bill follows below. Once again, we appreciate and commend this Subcommittee's efforts to gather public input and to hold this

hearing today. We hope the Subcommittee will move forward with those provisions of its bill and the Administration's bill that are non-controversial and responsive to the tragic attacks of September 11, but will defer on the other more complex and divisive provisions that we have identified. We look forward to working with the Subcommittee and staff to craft an appropriate response at this perilous moment in our country's history, and to avoid a rush to judgment on legislation that could ultimately imperil both freedom and security.

Extended Analysis of Administration Bill

The Administration's bill has two kinds of provisions that give rise to concerns: those that would lower the standards for government surveillance and those that address the difficult question of information sharing.

In terms of collection standards, our law enforcement and intelligence agencies already have broad authority to monitor all kinds of communications, including email. Both the criminal wiretap statute and the Foreign Intelligence Surveillance Act already cover terrorism. For some time, it has been recognized that those standards need to strengthen the standards for government surveillance. We see no justification for the changes proposed in the Administration bill that weaken those standards. We are particularly opposed to changes that would eliminate the judicial review that can be the most important protection against abuse.

The Foreign Intelligence Surveillance Act allows the FBI to conduct electronic surveillance and secret physical searches in the US, including surveillance of US citizens, in international terrorism investigations. FISA also authorizes court orders for access to certain business records. As you know, the standards under FISA are much lower than the standards for criminal wiretaps, and in return, the surveillance is supposed to be focused on the collection of intelligence, not criminal evidence. The FISA court, which last year approved more than 1000 surveillance requests, has denied only one request in its 22 year history.

Distinct from the Administration's unsupportable desire to avoid judicial controls on its authority, perhaps the central and most important problem facing the Congress is the question of information sharing. For many years, this has been recognized as a very difficult question; it is one that will be especially difficult to resolve satisfactorily given the pressure-cooker atmosphere of this time. We want to work out a balanced solution. But it cannot be done by wiping away all rules and barriers. Any solution needs to preserve the fundamental proposition that the CIA and other intelligence agencies should not collect information on US citizens in the US.

- **Section 101. Modification of Authorities relating to Pen Registers and Trap and Trace Devices**

Expands, in vague and potentially broad terms, the government's ability to get information about Internet communications under a loose standard. Also allows any magistrate in the country to issue a pen register or trap and trace order that can be served multiple times, anywhere in the country. – The government claims that it already has authority to collect, under the very weak provisions of the pen register and trap and trace statute, transactional data about Internet communications. But the existing statute, intended to collect telephone numbers, is vague as applied to the Internet. Section 101 compounds the vagueness. It would add the words “addressing” and “routing” to the description of what pen registers and trap and trace devices collect. What do these words mean?

We are concerned that the provision would be cited as expanding the scope of what the government collects, creating a more intrusive form of surveillance.

Internet addressing information can be much more revealing than phone numbers and might include information about the content of communications; a URL, for example, which may fit the proposed statutory definition of “addressing” information, may include a specific search term entered into a search engine or the title of a specific book bought at Amazon.com. The bill provides no details on how this content would be separated from other addressing information. *This provision is constitutionally suspect as it could allow government access to content information with minimal judicial oversight, specifically prohibited in a recent DC Circuit Court ruling. (See USTA v. FCC.)*

The standard for pen registers is so low as to be meaningless: people whose communications are targeted need not be suspected of any crime; probable cause is not required, only mere “relevance” to some ongoing investigation; courts have no authority to review these orders. Before extending nationwide scope to these orders, the process for their approval needs to be given some meaningful judicial approval. Congress now should use the language approved by the House Judiciary Committee last year in H.R. 5018.

- **Section 103. Authorized Disclosure**

Allows disclosure of information obtained from wiretaps with any executive branch official. This is clearly too broad, especially in light of the vague language in 18 USC 2517 that allows sharing when appropriate to the proper performance of the duties of the official **making** or receiving the disclosure. The issue of greatest concern to us is that the CIA and other intelligence agencies would begin compiling files on US persons. This provision should be narrowed, so that it authorizes disclosures to personnel with intelligence, protective, public health or safety, or immigration duties, to the extent that such disclosure is related to proper performance of the official duties of the officer receiving the disclosure, and with the proviso that nothing therein authorizes any change in the existing authorities of any intelligence agency. (Rather than amending the definition section of Title III, it might be better to build these concepts directly into section 2517.)

- **Section 105. Use of Wiretap Information from Foreign Governments. (Deleted from PATRIOT Act)**

Allows use of surveillance information from foreign governments, even if it was seized in a manner that would have violated the Fourth Amendment. Section 105 makes surveillance information collected about Americans by foreign governments (so long as U.S. officials did not participate in the interception) admissible in U.S. courts even if such interceptions would have been illegal in the U.S. Such a provision is ripe for abuse and provides unhealthy incentives for more widespread foreign surveillance of U.S. individuals; we commend its removal from the PATRIOT Act.

- **Section 106. Interception of Computer Trespasser Communications**

Allows ISPs to waive their customers privacy rights and permit government monitoring whenever customer violates terms of service. This provision says that a person accessing a computer system without authorization has no privacy rights. If an ISP’s terms of service prohibited use of the Internet account for illegal purposes, then the ISP could authorize government monitoring whenever the ISP was told by the

government that a customer might be doing something illegal. If a customer was suspected, for example, of downloading music that was copyrighted, the ISP could ask the government to monitor all the person's Web activities. This proposal would swallow the entire wiretap statute as applied to the Internet, relieving the government of ever having to get court approval to read e-mail.

- **Section 151. Period of Orders of Electronic Surveillance of Non-United States Persons Under Foreign Intelligence Surveillance.**

Allows secret searches and electronic surveillance for up to one year without judicial supervision. Under current law, the FISA Court can order a wiretap of a “non-US person” for a period of 90 days, after which the government must report to the court on the progress of the surveillance and justify the need for further surveillance. The court can authorize physical searches for up to 45 days. The amendment would extend both time frames to one year, meaning that after the government's initial ex parte showing there would be no judicial review for one year. We think this is too long. We recommend that the current time frames be retained for the initial approval. (After all, they are already far longer than the 30 days for which criminal wiretaps, including criminal wiretaps in terrorism cases, can be approved.) If, after 90- days of electronic surveillance or 45 days of physical searches, the government can show a continuing justification for the surveillance or search authority, then we would agree that the court could authorize a longer surveillance. We would recommend one year for electronic surveillance, 180 days for physical searches (thus preserving the current law's recognition that physical searches are more problematic than electronic searches and need to be authorized for shorter periods of time).

- **Section 152 Multi-Point Authority.**

Allows roving taps, including against US citizens, in foreign intelligence cases with no limits – ignoring the Constitution's requirement that the place to be searched must be “particularly described.” This section purports to afford the FBI “roving tap” authority for intelligence investigations similar to what already exists for criminal investigations. See 18 USC 2518(11). A roving tap allows the government to intercept whatever phone or email account a suspect uses, even if the government cannot specify it in advance. Roving tap authority is constitutionally suspect, at best, since it runs counter to the Fourth Amendment's requirement that any search order “particularly describe the place to be searched.” However, the proposed language places no limitation on the exercise of the roving tap authority and offers the FBI no guidance for its exercise. The proposed change merely authorizes the court to issue to any “person” an order commanding them to cooperate with a surveillance request by the government. If roving tap authority is supposed to focus on the targeted person, not on the telephone instrument, then the intercept authority should be limited to the target – it should only allow interception of communications to which the target of the surveillance is a party. Such limitations are absent from this proposal.

- **Section 153. Foreign Intelligence Information**

Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations -- an end-run around the relatively stringent

requirements for wiretaps in Title III. This section, which merely changes the word “the” to “a,” would actually make a fundamental change in the structure of the wiretap laws. It would permit the government to use the more lenient FISA procedures in criminal investigations which have any counter-intelligence purposes and would destroy the distinctions which justified granting different standards under FISA in the first place. Under existing law, FISA can be used only if foreign intelligence gathering is “the” purpose of the surveillance. The proposed provision would permit FISA’s use if this is “a” purpose, even if the primary purpose was to gather evidence for a criminal prosecution. This is an extraordinary change in the law which has no justification.

- **Section 154. Foreign Intelligence Information Sharing**

With no standards, permits the sharing of grand jury information, Title III wiretap information, and any other “foreign intelligence information” acquired in a criminal case with many different federal officials not involved in law enforcement. This is a sweeping change in the law. “Foreign intelligence information” is not defined. The provision places no limits on the purpose for which the information may be shared, and no limit on its reuse or redisclosure. It requires no showing of need and includes no standard of supervisory review or approval. As written, a criminal investigator could share with White House staff information collected about foreign policy critics of the Administration. The provision, at the very least, should be drastically curtailed.

- **Section 155. Pen Register and Trap and Trace Authority**

Eliminates the only meaningful statutory control that exists on use of pen register and trap and trace devices in intelligence cases. The law currently requires a showing that the person being surveilled is a foreign power, an agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities. This amendment would eliminate that standard and permit the use of FISA for pen registers whenever the government claimed that it was relevant to an ongoing intelligence investigation. Contrary to the DOJ’s assertion in its section-by-section, this is not the same as the standard for pen registers in criminal cases. There, the surveillance must be relevant to an ongoing criminal investigation, which is moored to the criminal law. There is no similar constraint on foreign intelligence investigations, since they can be opened in the absence of any suspicion of criminal conduct. This provision ignores the fact that the government was granted the special rules of FISA only for situations that involved intelligence gathering about foreign powers.

- **Section 156. Business records**

Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight. Traditionally, the FBI had no ability to compel disclosure of information in intelligence investigations. The compulsory authorities were limited to criminal cases, where the open, adversarial nature of the system offered protections against abuse. For example, in criminal cases, including international terrorism cases, the FBI can obtain grand jury subpoenas, under the supervision of the prosecutor and the court, where the information is relevant to a criminal investigation. The FBI has no ability to invoke the power of the grand jury in intelligence investigations, since those investigations are conducted without regard to any suspicion of criminal activity. In

1998, in an expansion of intelligence powers, FISA was amended to give the FBI a new means to compel disclosure of records from airlines, bus companies, car rental companies and hotels: Congress created a procedure allowing the FBI to go to any FISA judge or to a magistrate. The FBI had only to specify that the records sought were for a foreign intelligence or international terrorism investigation and that there were specific and articulable facts giving reason to believe that the person to whom the records pertain is an agent of a foreign power. This is not a burdensome procedure, but it brought the compulsory process under some judicial control. The Administration's bill would repeal the 1998 changes and permit the use of "administrative subpoenas" rather than an application to a court to get any business records under FISA. An administrative subpoena is a piece of paper signed by an FBI agent. There is no judicial review, no standard of justification, no oversight. Particularly in intelligence investigations, which are not even limited by the scope of the criminal law and in which there is no involvement of the US Attorney's Office, FBI agents should not have such unreviewable discretion to compel disclosure of personal information.

- **Sec. 157. Miscellaneous national-security authorities**
Allows much greater access to banking, credit, and other consumer records in counter-intelligence investigations. Current provisions of law allow the federal government to obtain sensitive banking, credit, and other consumer records under the relaxed and secretive oversight of FISA - but only when there are "specific and articulable" facts showing that the target consumer is "a foreign power or the agent of a foreign power." Section 157 would eliminate these essential requirements, mandating disclosure of this sensitive consumer data simply if an FBI official certifies that they are needed for a counterintelligence investigation (and with an ex parte court order for access to credit reports). Section 157 would eliminate the "agent of a foreign power" standard in—
 - The Fair Credit Reporting Act, allowing access to records from consumer reporting agencies (including the names of all financial institutions where accounts are held, all past addresses and employers, and credit reports);
 - the Financial Right to Privacy Act, broadly allowing access to financial records; and
 - the Electronic Communications Privacy Act, allowing access to telephone and toll billing records, and, newly added, all "electronic communication transactional records."As such, the Section would greatly increase access to the personal information of consumers or groups who are not agents of foreign powers. And in each case access to the institutions granting access to consumer information would be prohibited from disclosing that information or records had been obtained.
- **Section 158. Disclosure of educational records**
Amends the law protecting education records to permit access to them. While this might be justified in terrorism cases, the provision covers all cases involving "national security" and is far too sweeping.
- **Section 159. Presidential Authority.**

Does not appear to permit judicial challenge to seizure of property. At the very least, there must be such opportunity. A second provision allows the use of secret evidence. Use of such evidence, if ever permitted, must be on a much higher standard than that the information is properly classified, as provided here. The government must be required to persuade a court that the disclosure to the party would result in imminent and serious harm and the court must require the government to provide sanitized information to the party.

- **Section 352. Notice. Deleted from the PATRIOT Act.**

Allows secret searches of homes and offices. For any warrant or court order to search or seize property relating to a federal criminal offense, notice of the search or seizure could be delayed if it could interfere with lawful investigations. Notice is a bedrock Fourth Amendment protection from mistaken or abusive searches and seizures. Delayed notice has been allowed in only the most extraordinary circumstances, such as wiretapping, and only with substantial judicial supervision. Section 352 represents a major erosion of this key Fourth Amendment requirement of notice.