Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security

Oversight Hearing on Implementation of the USA PATRIOT Act: Sections of the Act that Address Crime, Terrorism, and the Age of Technology

April 21, 2005

Chairman Coble, Rep. Scott, Members of the Committee, thank you for the opportunity to testify at this important hearing. We want to commend the Subcommittee and the full Committee leadership for undertaking this series of hearings on the PATRIOT Act. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

Our main point today is that while, of course, the law needs to keep pace with changing technology to ensure that government agencies have access to information to prevent crime and terrorism, the law also needs to keep pace with changing technology to protect privacy, as technology makes ever larger volumes of information available for the government to acquire from third parties, without going to the subject of interest, as it used to have to do under the Fourth Amendment. The PATRIOT Act addressed only one side of this equation, making government access easier without counterbalancing privacy improvements. Now is the time for Congress to finish the job and address the privacy side of the equation.

In CDT's view, there are few if any provisions in the PATRIOT Act that are per se unreasonable. We see not a single power in the Act that should sunset. The question before us – and it is one of the most important questions in a democratic society – is what checks and balances should apply to those powers. With respect to the particular PATRIOT powers at issue in today's hearing, those time-honored checks and balances should include:

- Judicial review of intrusive techniques, preferably judicial approval before a search.

---

[1] 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. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

- Second, as a general rule, individuals should have notice when their communications are acquired by the government.

- Finally, government surveillance needs to be subject to Congressional oversight and some public accountability, including through more detailed unclassified reporting.

In one way or another, PATRIOT Act provisions fail to include these checks and balances.

Prevention of Terrorism Does Not Require Suspension of Standards and Oversight

At the outset, let me stress some basic points on which I hope there is widespread agreement:

- Terrorism poses a grave and imminent threat to our nation. There are people -- almost certainly some in the United States -- today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.
- These authorities, however, must be guided by the Fourth Amendment, and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

The Law Needs to Keep Pace with Technology – Both to Provide Appropriate Tools to Law Enforcement and to Protect Privacy

We have been told that this hearing will focus on three sections: 209 (misleadingly entitled "seizure of voice-mail pursuant to a warrant"); 217 (interception of computer trespasser communications); and 220 (nationwide service of search warrants for electronic evidence). Sections 209, 217 and 220 are not among the most controversial provisions of the PATRIOT Act. The fact that they are subject to the sunset at all, while, for example, the "sneak and peek" authority in Section 213 and the national security letter expansions in Section 505 are not subject to the sunset, illustrates how the debate over the sunsets is somewhat misplaced.

As with most other sunsetted provisions, there is little call for denying government the access to information provided under Sections 209, 217 and 220. Rather, the questions posed by these sections are matters of checks and balances, related to the continuing but uneven effort to rationalize the standards for government access to electronic communications and stored records in the light of ongoing changes in

technology. It is worth noting that Sections 209, 217 and 220 have no direct connection with terrorism. They apply to all criminal cases.

These sections highlight an overarching concern about the way in which amendments to the surveillance laws in recent years, and especially in the PATRIOT Act, have served as a "one-way ratchet" expanding government power without corresponding improvements in the checks and balances applicable to those powers. This has been a departure from Congress' traditional approach to electronic surveillance issues. In the first major wiretap statute, Title III of the 1968 Omnibus Crime Control Act; in the Electronic Communications Privacy Act of 1986; and even in the controversial Communications Assistance for Law Enforcement Act of 1994, Congress and the Justice Department agreed on the twin goals of ensuring law enforcement authority to intercept communications while also strengthening privacy protection standards, especially in light of changing technology.

This spirit of balance has unfortunately been lost. In recent years, time and again, the Department of Justice has proposed changes in the surveillance laws that reduce judicial oversight or increase Executive Branch discretion, and Congress has too often enacted them, without ever considering how these changes add up or whether other changes may be needed to increase privacy protections in response to advancements in technology that have made the government's surveillance more intrusive. Sometimes, as with the PATRIOT Act, this one-way expansion of government power occurs in a time of intense crisis. Sometimes, these changes occur stealthily, like the "John Doe roving tap" change that was added to FISA in December 2001 by the conference committee on the intelligence authorization act without having passed either the House or the Senate. Other one-sided and little debated expansions in the government's discretion include the expansion of ECPA's emergency disclosure authorities in the legislation creating the Department of Homeland Security, Pub. L. 107-296, Sec. 225(d). (That at least included a reporting requirement, which should be made annual.) A further exception to ECPA was made by Section 508(b) of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003, Pub. L. 108-21, which allowed disclosure without a warrant or subpoena of the contents of communications and subscriber identifying information to the National Center for Missing and Exploited Children, which in turn can disclose the information to law enforcement agencies. Changes to Title III's roving tap authority were adopted in the Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, Title VI, Sec 604, Oct 20, 1998, 112 Stat 2413 (permitting roving taps to be implemented if "it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communications will be or was transmitted"). And Section 731 of the 1996 anti-terrorism act excluded interception of wireless data transfers and of information about electronic funds transfers from the coverage of Title III.

Each of these changes is small in isolation, and each had a rationale. None, however, was considered in the context of other, long-recognized changes that need to be made to strengthen the privacy protections of the electronic surveillance laws, including:

- extending Title III's statutory suppression rule to electronic communications, a change even the Justice Department once supported;
- increasing the standard for pen registers and trap and trace devices, to give judges meaningful oversight, a change the full Judiciary Committee supported in 2000;
- eliminating the distinctions between opened and unopened email and between relatively fresh and older email, by bringing all stored email under a warrant standard, another change the Committee supported in 2000;
- establishing a probable cause standard for access to location information, a change this Committee also supported in 2000;
- requiring reporting on access to email, also supported by the Committee in 2000.

With this context in mind, it is easier to see why even some of the minor changes in the PATRIOT Act draw concern, for they are part of a steady stream of uni-directional amendments that are slowly eroding the protections and limits of the electronic privacy laws.

Section 209 – Seizure of voice-mail messages pursuant to warrant

Section 209 is described as permitting the seizure of voicemail messages pursuant to a search warrant. Previously, while voicemail messages stored on an answering machine in one's home could be seized by a search warrant, access to voicemail messages stored with a service provider had required a Title III order, which offers higher protections. The theory behind section 209 is that stored voice messages should be treated the same as stored data.

On one level, Section 209 makes the rules technology neutral, which is usually desirable. If Section 209 is taken at face value, and if the only difference it effects is between a Title III order and a search warrant, both issued on probable cause, Section 209 does not represent a big change. For this reason, CDT has described Section 209 as one of the non-controversial provisions of the PATRIOT Act.

However, as Prof. Swire points out, Section 209 is misleadingly titled: Because the law that was amended by 209 draws some bizarre distinctions between read and unread email and between newer and older email, Section 209 means that a lot of stored voice communications will be available not with a warrant but under a mere subpoena.

Moreover, the Justice Department's explanation of Section 209 overlooks the importance of notice under the Fourth Amendment and under Title III, and the absence of notice under the rules applied to stored material held by a service provider. When voicemail stored on your home answering machine is seized, you are normally provided notice at the time of the search. You can examine the warrant and immediately assert your rights. When email or voicemail is seized from a service provider pursuant to a warrant, you as the subscriber may never be provided notice unless and until the government introduces the information against you at trial. If you were mistakenly

targeted or the government chooses not to use the evidence, you need never be told of the search of your stored communications, so you have little meaningful opportunity to seek redress.

In the case of stored messages (whether email or voicemail), it is not even necessary from an investigative standpoint to deny contemporaneous notice in the way it is with live interception. Denial of notice is justified in the case of real-time interceptions because the effectiveness of the technique would be destroyed if the target were given contemporaneous notice. In the case of stored email or stored voice messages, the evidence is already created and, especially if notice is given immediately after seizure, the subject cannot destroy it. Denial of notice in the case of third party searches for stored email or voicemail is not justified.

Recommendation: Congress should take the Justice Department's description of Section 209 at face value, and make all seizure of stored communications, whether voice or email, subject to a warrant. It could do so by eliminating the difference between opened and unopened stored records and between records 180 days old or less and records more than 180 days old. It should take the Justice Department's arguments at face value and adopt truly technology neutral rules for voice and data, whether in transit or in storage, applying the protections afforded under Title III:

- minimization of non-relevant material,
- notice to persons whose communications have been intercepted,
- a statutory suppression rule, and
- detailed statistical reports to Congress and the public.

All of these protections apply to e-mail and voice when intercepted in transit. None of them apply to e-mail and voice seized from storage.

-- The Storage Revolution Is Rendering the Law Obsolete

A storage revolution is sweeping the field of information and communications technology. Service providers are offering very large quantities of online storage, for email and potentially for voicemail. Increasingly, technology users are storing information not in their homes or even on portable devices but on networks, under the control of service providers who can be served with compulsory process and never have to tell the subscribers that their privacy has been invaded. New Voice over Internet Protocol (VoIP) services may include the capability to store past voice conversations in a way never available before, further obliterating the distinction between real-time interception and access to stored communications.

Section 209 takes a seemingly small category of information out of the full protection of the Fourth Amendment and moves it under the lowered protections accorded to remotely stored communications and data. But stored voicemail is the tip of an iceberg. Increasingly, individuals are using stored email to store documents, including

draft documents on computers operated by service providers and accessed through a Web interface.

Rather than allowing growing amounts of personal information to fall outside the traditional protections of the Fourth Amendment, it is time to revisit the rules for networked storage (whether of voice or data) and bring them more in line with traditional Fourth Amendment principles, by requiring contemporaneous notice as the norm and covering both newer records and older records (again, whether voice or data) under the same probable cause standard. That would be truly technology neutral and would have the advantage of not allowing technology advances to erode privacy protections.

-- Section 217 – Interception of computer trespasser communications

Section 217 permits law enforcement agencies to carry out electronic surveillance of without a court order when the service provider permits the surveillance on the ground that a "trespasser" is using its system. Section 217 represents another in a steadily growing series of exceptions to the protections of the electronic communications privacy laws. (The emergency disclosure provision of Section 212 is another example.)

Section 217 and similar provisions essentially allow "off the books surveillance" – they define certain interceptions not to be interceptions, and certain disclosures not to be disclosures. Once an access to communications or data is excluded from the coverage of the surveillance laws, not only is it not subject to prior judicial approval, but also there are no other protections normally associated with electronic surveillance:

- There is never a report to a judge. (In contrast, under both Title III and FISA, when electronic surveillance is carried out on an emergency basis, an application must be filed after the fact.)
- There is no time limit placed on the disclosures or interceptions. (A Title III wiretap cannot continue for more than 30 days without new approval.)
- There is never notice to the person whose communications are intercepted or disclosed.
- There is no statutory suppression rule if the communications were improperly seized, and there would be no suppression remedy at all if the information is deemed to be outside the protection of the Fourth Amendment.
- The interceptions and disclosures are not reported to Congress or the public.

The Department of Justice, in its defense of Section 217, claims that the privacy of law-abiding computer users is protected because only the communications of the computer trespasser can be intercepted. But what if the system operator is wrong? What if there is a legitimate emergency, but law enforcement targets the wrong person? Under Section 217, a guilty person gets more notice than an innocent person – the guilty person is told of the surveillance or disclosure but the innocent person need never be notified.

Contrary to the Department's arguments, Section 217 is not analogous to the case of the home trespasser. While the homeowner can invite in the police onto his property,

the homeowner cannot authorize the police to go through the trespasser's pockets or read the papers in his briefcase. To do so requires a separate Fourth Amendment basis, which would require a warrant unless one of the exceptions applied, and in the online context, there may be no other exception available.

Recommendation: While an emergency exception to the court order requirement may be appropriate for trespasser situations, interceptions under the trespasser rule should be treated as interceptions under Title III:

- As with other emergency interceptions, when electronic surveillance is carried out on an emergency basis, an application for judicial approval must be filed after the surveillance commences
- The length of interceptions should be limited to the time necessary to identify the trespasser or for 30 days, whichever is less
- Interceptions under the trespasser rules should be treated as interceptions for purposes of giving delayed notice to the person whose communications are intercepted.
- Interceptions under the trespasser rules should be treated as interceptions for purposes of the statutory suppression rule.
- Interceptions under the trespasser rule should be counted as interceptions for Title III purposes and included in the annual Wiretap Report.

-- Section 220 – Nationwide service of search warrants for electronic evidence

Section 220 amended 18 U.S.C. 2703 to allow judges to issue search warrants for electronic evidence that can be executed outside of the district in which the issuing court is located. In a world where the center of an investigation may be in one state, but the target's ISP has its servers in another state, this makes obvious sense. Moreover, unlike Section 216, which authorizes a kind of roving pen register (one order can be served on multiple service providers in different districts until the government gets the full picture it wants), it seems that search warrants under Section 220 have to name the service provider upon whom they will be served. If it turns out that that provider does not have the records being sought, the government will have to obtain a new search warrant (as it would any time a search warrant does not turn up the expected evidence.)

However, as the Electronic Privacy Information Center has noted, Section 220 removes "an important legal safeguard by making it more difficult for a distant service provider to appear before the issuing court and object to legal or procedural defects. Indeed, it has become increasingly common for service providers to seek clarification from issuing courts when, in the face of rapidly evolving technological changes, many issues involving the privacy rights of their subscribers require careful judicial consideration. The burden would be particularly acute for smaller providers."

Recommendation: One solution to this problem is to allow a warrant to be challenged not only in the district in which it was issued but also in the district in which it

is served. While the issuing judge may have a better sense of the factual basis for the order, a judge in the district in which the order is served may be in a better position to interpret or redefine the scope of the order in light of issues concerning the system of the service provider on whom the order is served.

Even aside from Section 220, whether search warrants for electronic evidence are issued for evidence inside or outside their jurisdictions, judges should question applicants to be sure that the warrant is narrowly drawn. Judges should use extra care in understanding what information is being sought, whether it will be copied or originals will be seized (interfering with ongoing business), and whether it is possible to disclose just certain fields or just records from a certain pertinent timeframe. These are analogous to questions that judges have the authority to consider in the case of physical searches, but judges need to understand computer systems in order to fully enforce the specificity requirement of the Fourth Amendment in the digital context. Judges should look more carefully at the return of service. While notice under 18 U.S. C. 2705(b) can be prohibited, judges should be hesitant to deny notice to the person to whom the records pertain, since the subscriber is really in the best position to raise legitimate concerns. This is just another way in which judges faced with the authorities of the PATRIOT Act can assert closer scrutiny and place conditions on the exercise of PATRIOT authorities without denying the government access to the information needed.

Conclusion

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

We look forward to working with this Subcommittee and the full Committee as you move forward in seeking to establish some of the checks and balances that were left behind in the haste and anxiety of October 2001.

For more information, contact:
Jim Dempsey
(202) 637-9800 x112
http://www.cdt.org