



September 28, 2001

**Analysis of Key Anti-Terrorism Bills
Introduced After September 11, 2001**

In response to the September 11, 2001 terrorist attacks, several legislative packages are circulating on Capitol Hill that seek to address the Bush Administration's request for expanded surveillance powers. The key proposals being circulated are bills by the Administration ("Anti-Terrorism Act of 2001"), by Senate Judiciary Committee Chair Patrick Leahy ("United and Strengthening America Act"), and by Senate Intelligence Committee Chair Bob Graham (S. 1448, the "Intelligence to Prevent Terrorism Act of 2001"). Both Judiciary Committees and the Senate Intelligence Committee held hearings this week on the proposals, and voting by the committees is expected soon.

The surveillance provisions would primarily amend the federal wiretap laws (18 U.S.C. §§ 2510, 2701, 3121 et seq.), used for domestic surveillance in criminal investigations, and the Foreign Intelligence Surveillance Act ("FISA"), used for domestic surveillance of non-Americans in counter-intelligence investigations. Although these draft bills also propose amending the immigration laws, the money laundering statutes, and other laws, this memorandum only summarizes key aspects of the surveillance provisions of greatest interest to Internet service providers and other communications service providers.

The bills propose less restrictive standards for surveillance and for sharing of information among law enforcement and intelligence agencies. Because some of these proposals have been hastily drafted, and are being pushed quickly with little time for debate, they may have an impermissible impact upon civil liberties as well as increase the risks of liability for service providers. Another effect of the proposals would be an increase in requests for surveillance, which would make it increasingly difficult for service providers to fully comply with law enforcement requests. In addition, the proposals raise questions about design and data retention mandates. More specifically, although the bills do not contain language explicitly requiring service providers to retain customer information, to design or configure their systems in particular ways, or otherwise to undertake any action that exceeds their existing technical capabilities, the proposals implicitly raise questions whether courts will interpret the legislation as requiring the judiciary to ensure that the information the government would now have the power to request is in fact available from service providers. . But there is also a risk that adding specific statutory language seeking to make clear that neither existing law nor the new legislation imposes any technology design mandates, or requires the installation of Carnivore in any or specified situations, could create a negative implication about the *status quo*.

These concerns should not overshadow the importance of many of the proposals and the fact that many of them contain provisions welcomed by industry. For example, the Administration's Bill proposes enabling service providers victimized by computer trespassing to request law enforcement assistance in monitoring hacking attacks as they occur, clarifying the issue of what law applies to surveillance requests served upon cable operators providing Internet or other communication services, and resolving an ambiguity in current law that inhibits service providers from disclosing customer information in emergency situations involving death or serious physical injury. But the actual proposals need to be reviewed to ensure that they do not create additional or unnecessary problems for industry.

The remainder of this memorandum discusses these issues and the provisions that give rise to them.

For more information, contact Ron Plessner, Jim Halpert, or Milo Cividanes at (202) 861-3900.

I. Proposals that could increase the risk of liability for ISPs

A. Nationwide Service for Pen Register Orders

Description: Section 101 of the Administration's Bill would authorize courts to grant pen register/trap and trace orders that are valid "anywhere within the United States." Under current law, for every pen register/trap and trace device it wants installed, the government must apply for a court order in the jurisdiction in which the service provider is located. Both this proposal and Section 204 of Senator Leahy's bill would add a sentence stating that, upon service of such court order, the order shall apply to any person "providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." As described by the government: "This amendment would increase tracing efficiency by eliminating the current need to apply for new orders each time the investigation leads to another jurisdiction."

Implications: Companies served with the new nationwide pen register/trap and trace orders could face increased liability risks. Although the statute does not currently require such orders to specify the service providers upon whom they are served, as a practical matter such orders do name the service provider and the subscriber service that is under surveillance. The advent of nationwide service will result in providers being asked to render assistance even though the provider is not specifically named in the order and the assistance that is being requested is not specifically defined in the order. Of particular concern here, the specific assistance may be orally transmitted by the investigating agent. This makes it harder to demonstrate subsequently that the service provider has acted in good faith or that the law enforcement agents are the source of any errors.

B. Authorizing the Interception of Computer Trespasser Communications

Description: Section 106 of the Administration’s Bill would authorize persons “acting under color of law” to intercept the communications of trespassers upon protected computers when the owner or operator of the computer authorizes such monitoring. It would enable service providers victimized by computer trespassing to request law enforcement assistance in monitoring hacking attacks as they occur.

Implications: Although this proposal would protect law enforcement when engaging in such monitoring, it does not appear to protect the owner or operator of a protected computer from liability for authorizing the interception, for example, if it errs in good faith in identifying the trespasser. Granting service providers protection from liability by the target of the investigation is consistent with other immunities in the wiretap statute and essential if companies are to work with law enforcement as envisioned by Section 106.

C. Applying the Wiretap Laws to the Surveillance of Certain Cable TV Customers

Description: The Cable Act requires operators of cable television service to notify affected subscribers of any court order compelling surveillance or of the production to the government of customer records, and establishes certain evidentiary and procedural hurdles to a court’s issuance of such orders. The wiretap laws governing the disclosure of the records or the monitoring of the communications of the customers of Internet service providers and telephone companies do not contain these conditions and requirements. Cable operators providing Internet or other communication services face a dilemma when served with lawful surveillance requests issued under the wiretap laws rather than under the Cable Act, and have often refused to comply with such requests. Section 109 of the Administration’s Bill would relieve cable operators of this dilemma by stating that nothing contained in the Cable Act “shall be deemed to restrict” disclosures of information under the wiretap laws, but exempting from this override of the Cable Act any disclosures of information “revealing customer cable television viewing activity.”

Implications: Cable operators providing Internet or other communication services probably will welcome changes in the law that clarify in a definitive manner what law they must comply with when served with lawful surveillance requests: the Cable Act or the wiretap laws. However, by being couched in terms of “restrictions” rather than “conditions,” section 109’s language does not completely override the Cable Act in these circumstances. In addition, the “viewing activity” exception to the override thrusts a cable operator served with a lawful surveillance request issued under the wiretap laws back into the jurisdiction of the Cable Act. In short, section 109 does not accomplish its objective and exposes cable operators to liability they do not currently face.

D. Increased Need for Immunity for Helping Effectuate Wiretaps under FISA

Description: Section 152 of the Administration’s Bill, Section 207 of Senator Leahy’s Bill, and Section 203 of Senator Graham’s Bill would authorize roving wiretaps under FISA by allowing the government to serve an order on multiple providers where the FISA Court “finds” that “the actions of the target” of the electronic surveillance could/may “have the effect of thwarting” (Leahy/Administration) or “may thwart” (Graham) the identification of the appropriate provider. These proposal are intended to address what the new FBI Director described as the need for authority to wiretap “an individual regardless of whether he buys a cell phone on day one and a week later buys another cell phone with another number and moves from cell phone to cell phone seeking to avoid interception. That’s a key piece of legislation that would be very helpful to us in monitoring conversations of those we suspect or know to be terrorists.”

Implications: Roving taps have been authorized under the wiretap laws, but not under FISA, since 1986. A roving tap authorizes law enforcement to intercept *all* of its suspect’s wire or electronic communications relating to the crime under investigation, regardless of the suspect’s location when communicating. The quintessential situation requiring a roving wiretap is when a suspect goes from phone booth to phone booth numerous times in an effort to prevent his calls from being wiretapped. But, when faced with a suspect that frequently uses different Internet accounts with various ISPs, the existing and new authority could be used to obtain a court order issued to various ISPs instructing them to implement surveillance on any account that law enforcement believes the target may be using at a particular point in time.

However, whereas every other surveillance law (including FISA’s pen register/trap and trace provisions) contains a good faith immunity clause that protects ISPs from liability for any assistance they render the government in compliance with an order, in an apparent oversight the FISA wiretap provisions do not contain a similar provision. With an anticipated increase in FISA wiretaps, it is important that this oversight be corrected in this bill.

II. Proposals that could increase burdens upon ISPs

A core element of the Administration’s efforts is to streamline the processes for conducting surveillance. The Administration asserts that some surveillance tools are rarely used because of procedural obstacles (e.g., pen register and trap and trace devices under FISA), or not used as much because of the substantial delays associated with using them (e.g., National Security Letters). Mere changes that will make it easier for the government to use these surveillance tools will cause a concomitant increase in compliance costs for service providers. But other changes, summarized below, could create obstacles to the way service providers currently respond to requests for surveillance assistance, as well as increase burdens upon them.

A. Application of Pen Registers to Internet Communications

Description: Section 101 of the Administration’s proposal would make clear that the pen register and trap and trace statute extends to all routing information related to Internet communications, rather than just number dialed. This would be accomplished primarily by changing the definitions of pen registers and trap and trace devices to reflect their ability to capture “dialing, routing addressing, and signaling information” transmitted by a facility from which wire or electronic communications are transmitted. Section 204 of the Leahy proposal also would extend the pen register and trap and trace statute to Internet communications, but would limit the information to be captured by these devices to signaling information utilized in “identifying the origination or destination of wire or electronic communications.”

Implications: Although the government’s witnesses at congressional hearings have indicated that they seek only clear authority to obtain the “to” and “from” header information in e-mail communications, the likely effect of the Administration’s proposal would be to require ISPs to track other Internet-related information, such as chat room discussions and web surfing—information that, in many cases, ISPs are not currently tracking or storing in a retrievable format. In addition, by using the term “signaling information,” which is also found in CALEA’s (the Communications Assistance for Law Enforcement Act) definition of “call identifying information” (CII), the Administration’s proposal could adversely affect the pending proceeding in which the Federal Communications Commission is to determine whether telecommunications carriers must design their systems in order to provide certain features requested by the FBI (the so-called “punch list items”) because the information they generate supposedly falls within the definition of CII. The Leahy proposal appears to be more narrowly focused and more likely to achieve only the goal articulated by the Administration. Under either proposal, service providers are likely to see increased requests for Internet-related information.

B. Nationwide Service for Certain Court Orders

Description: As discussed above at I.A, both the Administration’s Bill (Section 101) and the Leahy proposal (Section 204) would provide courts with the authority to issue pen register and trap and trace orders that can be served on service providers nationwide.¹ In addition, Section 108 of the Administration’s proposal would provide for nationwide service of process of

¹ The Administration’s proposal would retain the current low evidentiary standard that merely requires a government attorney to certify that the information likely to be obtained is likely to be relevant to an ongoing criminal investigation, and the low procedural standard that calls upon a judge to only verify that the government attorney has made the requisite certification and signed the application. By contrast, the Leahy proposal would provide for a greater adjudicative role by requiring court confirmation of a factual basis that the information likely to be obtained is relevant to an ongoing criminal investigation.

search warrants for stored communications, such as e-mails, and other records relating to online and voice mail accounts.

Implications: Nationwide service, particularly of search warrants, could make it very difficult for local or regional service providers to oppose, modify, or contest warrants or court orders. For example, an ISP in California that would ordinarily be able to seek a hearing with the local federal court to raise any issues it might have with the court order which had been served upon it, might now have to hire counsel in New York and fly witnesses to the East Coast to accomplish the same task before the federal court in New York that issued the court order. In short, this provision could require service providers to travel to numerous courts, in multiple jurisdictions, to address concerns over the breadth of court orders and search warrants.

C. Subscriber Records

Description: Section 107 of the Administration’s bill would make new categories of information (e.g., records of “session times and durations”) subject to disclosure by subpoena. Currently, only information about subscribers, not their transactions, is available by subpoena from ISPs. This would require ISPs to produce certain transactional information in response to a subpoena rather than a court order.

Implications: This would expand the categories of subscriber information that the government can obtain from service providers with a subpoena to include both “records of session times” and identification of “any temporarily assigned network addresses.” Providers can expect to see increased requests for this detailed information relating to subscribers of their services.

D. Compensation for Backup Preservation Requests

Description: As the Administration’s proposal makes it easier to serve warrants in multiple jurisdiction and otherwise conduct surveillance, a discrepancy in existing law could prevent service providers from obtaining reimbursement for reasonable costs incurred complying with governmental requests to preserve information. Under current law, the government may request a service provider to create backup copies of the requested information. However, service providers are entitled to reimbursement only for information “obtained” by the government. Service providers could get saddled with the cost of preserving data that is never disclosed to the government (for example, because the government drops the investigation).

Implications: Compliance with these surveillance requests can be very burdensome. The general rule is that providers are entitled to reimbursement for complying with government requests under federal surveillance laws. If the opportunity is not taken now to clarify the issue of reimbursement costs for backup preservation regardless of delivery, service providers could be required to collect and store—with no compensation—voluminous amounts of information that they may not normally maintain in the normal course of business.

E. FISA Business Records

Description: Section 156 of the Administration's bill would amend FISA to allow the Federal Bureau of Investigations to require, by administrative subpoena, "the production of any tangible things (including books, records, papers, documents, and other items) that are relevant to the investigation."

Implications: To the extent that these modifications make government investigations easier, ISPs can expect an increase in the volume of requests for assistance.

III. Technology design or data retention mandates

In identifying new categories of information to be produced by an ISP and otherwise proposing to make it easier for government to conduct surveillance, the question arises whether with these new surveillance powers comes the corresponding obligation by ISPs to acquire equipment or reconfigure their systems in particular ways to ensure that the information the government now has the power to request is in fact available from service providers.

For example, with a court order for a roving tap, law enforcement may furnish a service provider only with an individual's name and ask for surveillance to be conducted on all separate telephone or e-mail accounts linked to the name. This linkage of separate accounts to a name may not be a normal business practice. To respond to these types of requests on an ongoing basis, a service provider may need to reprogram its system to link similar names across accounts—a requirement that would result in the development of a tracking database. Another example would arise if the amendments to the pen register and trap and trace statutes were to authorize the tracing of a broad range of Internet communications beyond e-mail communications, such as past chat room discussions and web surfing. Although ISPs may have the capability to assist in surveillance in connection with chat room and web surfing activities that take place after being served with a court order, they would not have such information for activities preceding service of an order because their business practices may not call for storing of subscriber information. Moreover, questions arise as to whether the final legislation will be interpreted to authorize the government to insist on the installation of DSC-1000 (Carnivore) in situations where ISPs are unable to respond immediately to government requests.

In a 1994 committee report carefully vetted by the FBI, the Judiciary Committees noted that a review of the wiretap statutes and the case law on the inherent powers of the judiciary to effectuate court orders revealed that the issue of whether communications service providers have the obligation to design their systems such that they do not impede law enforcement surveillance has never been formally adjudicated. (This is why the two Judiciary Committees recommended passage by Congress of CALEA, which does not apply to ISPs.) But, our own independent review of past case law reveals that neither statutory nor non-statutory authorities allow the

government to require *before-the-fact* action by service providers to assist in the surveillance of *future, theoretical* targets. On the contrary, these authorities require the government to make a particularized showing regarding the specific target of the interception, and reveal courts assessing the burdens of the government's requests in relation to the companies' *existing* technical capabilities. They also establish that the government must fully compensate service providers for the cost of assistance when tailoring their facilities to meet the needs of a particular request. Supreme Court case law on the protections afforded by the Constitution's "takings clause" since these surveillance cases were decided only underscore the hurdles facing the government if they argue at some future date that with these new surveillance powers comes the corresponding obligation by ISPs to reconfigure their systems to assist in the surveillance of future, theoretical targets.

This view of the *status quo* should give pause to any effort by industry to add specific statutory language seeking to make clear that neither existing law nor the new legislation imposes any technology design mandates or requires the installation of Carnivore in any or specified situations. Such language could create a negative implication about the *status quo*.

IV. Other Proposals

Emergency Disclosures by Service Providers

Description: Section 110 of the Administration's proposal would authorize service providers to disclose the content of stored e-mail messages and other customer information where the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information."

Implications: There is no express provision in existing law permitting service providers to make such emergency disclosures. This would help resolve an ambiguity in current law that inhibits service providers from disclosing customer information in emergency situations involving death or serious physical injury.