

Commercial Internet eXchange (CIX)

Stewart Baker (outside counsel for CIX)

Steptoe & Johnson LLP

(202) 429-6413

sbaker@steptoe.com

Anti-Terrorism Act of 2001: Analysis & Proposed Modifications

Several parties have analyzed the potential civil liberties implications of the Administration's Anti-Terrorism Act that is currently pending before Congress.

The Commercial Internet eXchange ("CIX") has been asked to examine the practical implications of the Administration's anti-terrorism legislation for Internet service providers. ISPs have a long history of working cooperatively with law enforcement authorities in complying with the federal surveillance laws, and are ready to assist law enforcement with the implementation of any anti-terrorism legislation passed by Congress. By and large, CIX concludes, the Administration's bill has been drafted with some sensitivity to the concerns of ISPs. For example, the provision that allows ISPs to voluntarily disclose information when they believe that there is a threat of death or serious injury would resolve a current ambiguity in federal surveillance law that has caused unnecessary concern for ISPs responding promptly to genuine emergencies.

However, there are a variety of small modifications that would strengthen the effectiveness of the legislation for both law enforcement and ISPs. We believe that the following proposed modifications, largely patterned after comparable provisions in existing federal surveillance statutes, would meet those goals, by:

- Exempting service providers from liability for assistance rendered to the government in good faith compliance with the Act's provisions;
- Clarifying that no new technology mandates are imposed by the legislation and that service providers may comply with pen register/ trap and trace orders using their own internal capabilities; and
- Clarifying that ISPs should receive reimbursement for the reasonable costs of complying with government preservation orders and billing record requests.

1. Good Faith Immunity for Complying with Surveillance Requests

A. Roving Pen Register/Trap and Trace Authority (Section 101)

Proposal: “Section 101(b)(1) is amended at the end after ‘execution of the order,’ by striking the period and inserting:

‘in the United States, provided that if the order is served on any person or entity not specifically named in the order, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide a written statement, addressed to the person or entity, specifying the assistance to be provided by the person or entity under the terms of the order.’”

Explanation: *First, Section 101 is ambiguous as to whether a U.S. provider may be required to perform assistance outside the United States. Although the bill refers to service providers “in the United States,” it does not clarify whether “the execution of the order” (when applied to a provider that offers both domestic and international services) is similarly limited to assistance within the United States. This modification would clarify the perceived intent of the provision and is consistent with existing provisions of the Electronic Communications Privacy Act (ECPA), which are limited to the U.S.*

Second, as a result of the expanded multi-point surveillance authorities provided in the Administration’s bill (for example, Section 101), providers will be 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, the specific assistance may be orally transmitted by the investigating agent. In this situation, to protect themselves from potential liability, providers should have proof of what the agent requested. Requiring the agent to provide such requests for assistance in writing would minimize the risk for error and help document, for purposes of the provider’s “good faith” immunity, what assistance was requested.

B. Roving Pen Register/Trap and Trace Authority (Section 101 – con’t)

Proposal: “Section 101 is amended by inserting a new subsection (d) as follows:

‘(d) IMMUNITY – Section 3124(d) of title 18, United States Code, is amended by striking ‘the terms of’ after ‘information, facilities, or assistance in accordance with.’”

Explanation: *This is a conforming change to keep pace with the “roving” orders authorized by the Administration’s bill. Because these orders would not necessarily specify the companies that must comply with the order, the corresponding immunity provision for pen register/trap and trace orders, 18 U.S.C. § 3124(d), needs to be updated to resolve any doubt that providers who are not named in the court order are nonetheless protected from liability for complying with the order. The current language of § 3124(d) protects providers only if they provide assistance “in accordance with the terms of a court order.” The phrase “the terms of” is unnecessary and may suggest that*

providers complying in good faith with the expanded “roving” authority may be ineligible for the § 3124(d) protection unless they are named in the order itself.

C. Interception of Computer Trespasser Communications (Section 106)

Proposal: “Section 106 is amended by adding a new paragraph (3) as follows:

‘(3)(a) Section 2520(d) of title 18, United States Code, is amended by inserting a new paragraph (4) as follows:

‘(4) a good faith determination that a person is a computer trespasser whose communications the owner or operator of a protected computer may authorize to be intercepted under section 2511(2)(i).’

(b) Section 2511 of title 18, United States Code is amended by inserting a new subsection (j) as follows:

‘(j) No cause of action shall lie in any court against any owner or operator of a computer, its officers, employees, or agents, in connection with the authorization pursuant to this section of any person acting under color of law to intercept communications of someone believed to be a computer trespasser.’”

Explanation: *Although Section 106(2) of the Administration's proposal would protect law enforcement when an owner or operator of a protected computer authorizes the interception of the communications of a trespasser, it does not appear to protect the owner or operator from liability for authorizing such an interception, for example, if it errs in good faith in identifying the trespasser. Such protection from liability is consistent with ECPA and essential if companies are to work with law enforcement as envisioned by Section 106.*

D. Emergency Disclosures of Customer Information (Section 110)

Proposal: 1. “Section 110 is amended by adding a new subsection (c) as follows:

‘(c) Section 2702 of title 18, United States Code, is amended by adding after subsection (c) a new subsection (d) as follows:

‘(d) No cause of action shall lie in any court against any provider of electronic communication service or remote computing service, its officers, employees, or agents in connection with voluntary disclosure of customer communications or records pursuant to subsection (c).’”

2. “Section 110(a)(5)(C) is amended by striking the words ‘reasonably’ and ‘immediate.’”

Explanation: *Although Section 110 of the Administration bill would authorize ISPs to disclose customer information when there is a serious risk of personal injury or death, it does not appear to protect the owner or operator from “good faith” mistakes that might be made by an ISP. Consistent with other federal statutory provisions, a good faith immunity clause should apply to ensure that fear of liability does not deter an ISP from making the emergency disclosure authorized in this section. Similarly, the word “immediate” should be removed as a service provider may not know when a harm will take place.*

E. FISA Wiretap Immunity (new Section 160)

Proposal: Insert a new Section 160 as follows:

“SEC. 160 Good Faith Compliance with FISA Wiretap Authority”

Section 1805 of title 50, United States Code, is amended by adding after subsection (g) the following new subsection:

‘(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with the terms of a court order or request for emergency assistance under this chapter.’”

Explanation: *Every other surveillance law (i.e., Title III, ECPA, FISA pen register/trap and trace) contains a good faith immunity clause that protects ISPs from liability for any assistance they render the government in compliance with an order. However, in an apparent oversight the FISA wiretap provisions do not contain a similar provision. This oversight should be corrected in this bill. The proposed immunity clause for FISA wiretaps is modeled on the similar immunity already provided for FISA pen register/trap and trace orders (50 U.S.C. § 1842(f)).*

2. Reimbursement of Costs

A. Reimbursement of Costs for Preservation Requests (new Section 111)

Proposal: Insert a new Section 111 as follows:

“Sec. 111. – Section 2706(a) of title 18, United States Code, is amended by striking ‘governmental entity obtain’ and inserting ‘governmental entity requesting the disclosure or preservation of.’”

Explanation: *Section 2706 is ambiguous regarding whether providers should receive reimbursement for reasonable costs incurred complying with obligations to preserve information that is never disclosed to the government (for example, because the government drops the investigation or never obtains an appropriate order). These requests can be very burdensome. Providers are entitled to reimbursement for complying with all other government requests under federal surveillance laws. Because § 2706(a) permits reimbursement only of costs that have been “directly incurred” in complying with the government surveillance request. Therefore, providers will not receive compensation under this amendment if the government requests information, but the provider does not in fact incur costs taking action in response to the government request.*

B. Reimbursement of Costs for Billing Records (new Section 112)

Proposal: Insert a new Section 112 as follows:

“Sec. 112. – Section 2706 of title 18, United States Code, is amended by striking subsection (c).”

Explanation: *Providers are entitled to reimbursement for complying with all other government requests under federal surveillance laws, except under section 2706(c) when complying with government requests for basic subscriber and billing records. Congress originally adopted this exception, in part, because they did not expect compliance with such requests to be particularly burdensome. In practice, however, these requests have become the most common requests for assistance received by most providers and, as a whole, the volume of these requests can be very burdensome. Providers have to devote large staffs to complying with these requests.*

3. Technical Assistance

A. Pen Register/Trap and Trace Authority (Section 101)

Proposal: “Section 101(b) is amended by adding a new paragraph (3) as follows:

‘(3) Nothing in this chapter shall authorize the government to demand the installation of a government-owned pen register or trap and trace device or the use of a specific technical capability if the entity or person on whom an order is served can otherwise comply with the order.’”

Explanation: *This modification preserves current law and practice by clarifying that ISPs may comply with pen register/trap and trace orders using their own technology, rather than being required to install a particular, government-mandated technology (such as Carnivore). The current language of 18 U.S.C. §3123(a), as amended by Section 101, could be inadvertently interpreted as allowing law enforcement to mandate the installation of a particular device, even though the service provider may be able to comply with the order using its own internal capabilities.*

B. No Technical Mandate (new Section 161)

Proposal: Insert a new Section 161 as follows:

“Sec. 161. – Assistance to Law Enforcement Agencies. Nothing in this Act shall impose any technical obligation or requirement on a provider of wire or electronic communication service or other person to modify their equipment, facilities or services in order to furnish facilities, services or technical assistance. A provider of a wire or electronic communication service or other person who furnishes facilities, services, or technical assistance pursuant to this Act shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities, services, or assistance.”

Legislative History: Include report language explaining that the Anti-Terrorism Act does not impose any technical mandate upon service providers:

“These amendments do not change the traditional scope of a service provider’s obligation to provide technical assistance and otherwise assist law enforcement in effectuating authorized electronic surveillance, which is governed by 18 U.S.C. 2518(4) and other similar provisions elsewhere in titles 18 and 50. These statutory provisions have been interpreted by the courts to require service providers and others served with requests for assistance in effectuating lawful surveillance to provide only information available at the time of the request or information available using their existing technical capabilities. It is the intent of the Committee that the Anti-Terrorism Act of 2001 does not create new obligations for service providers to store customer information, to design or configure their systems in particular ways, or otherwise to undertake any action that exceeds their existing technical capabilities.”

Explanation: *The traditional scope of a service provider’s obligation to provide technical assistance and otherwise assist law enforcement in effectuating authorized electronic surveillance has been well defined by the courts (including the Supreme Court in its decision in United States v. New York Telephone) and other federal statutes. This modification would clarify that nothing in this Act changes these existing obligations.*

4. Other Clarifications

A. Require Written Preservation Orders (new Section 113)

Proposal: Insert a new section 113 as follows:

“Sec. 113 – Section 2703(f)(1) of title 18, United States Code, is amended by adding the word ‘written’ after the word ‘the’ and before the word ‘request.’”

Explanation: *Although the Justice Department has adopted a policy that all preservation requests should be confirmed in writing, federal law is silent on whether preservation orders may be verbal. Both ISPs and law enforcement would benefit from a statutory requirement of written notice, which would minimize the possibility of mistakes.*

B. Require Preservation Orders to Identify with Particularity the Records to be Preserved (new Section 114)

Proposal: Insert a new Section 114 as follows:

“Sec. 114 – Section 2703(f) of title 18, United States Code, is amended by adding a new paragraph (3) as follows:

‘(3) Identification of records – Requests referred to in paragraph (1) shall identify with particularity the records to be preserved.’”

Explanation: *A particularity requirement would enable ISPs to respond promptly and specifically to the concerns of the requesting governmental entity.*

C. Define What is Meant by “Addressing and Routing Information”

Proposal: This bill should define what is meant by “addressing and routing information” to clarify that this term does not include content such as URLs or subject lines.

Explanation: *There is no definition for “addressing and routing information” under the Administration’s current proposal. However, these are rather broad terms that could inadvertently encompass the content of a subject’s communications, such as URLs or subject lines. The Justice Department does not currently consider URLs, subject lines or other content to be covered by the pen register/trap and trace provisions of ECPA and has indicated that it does not intend its amendment to broaden these provisions beyond this current understanding. Adding a narrow definition of “addressing and routing information” that confirms that it does not include content would be consistent with the Justice Department’s intent.*