KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CONCERNS WITH "MONITORING" AND "COUNTERMEASURES" LANGUAGE IN THE SENATE CYBERSECURITY BILL*

September 10, 2012

CDT is concerned that the monitoring and countermeasures language in Section 701 of the Senate cybersecurity bill, S. 3414, is overbroad, especially when read in conjunction with the bill's immunity language (Section 706). We urge the bill's sponsors and all stakeholders to work together to develop more focused language that would address specific problems in current law. In the meantime, should the bill be taken up this Fall, we would support an amendment offered by Senators Franken and Paul to strike Section 701.

The lead Senate cybersecurity bill (sponsored by Senators Lieberman and Collins) has a provision, Section 701, stating that any private entity may monitor its information systems and information that is stored on, processed by, or transiting such information systems and may operate "countermeasures" on its information systems to protect its rights or property from cybersecurity threats. Section 701 also authorizes any private entity, with consent, to monitor and perform countermeasures on the system of a third party. The provision authorizes monitoring and countermeasures "notwithstanding" the major federal laws that protect the privacy of communications. The Administration's proposed cybersecurity legislation included no monitoring or countermeasures language.

CDT is concerned that the monitoring and countermeasures language is overbroad, especially when read in conjunction with the bill's immunity language (Section 706). We would like to work with the bill's sponsors and with industry and other interested parties to develop more focused language that would address specific problems in current law. In the meantime, we are supporting the amendment offered by Senators Franken and Paul to strike Section 701. Although the Lieberman-Collins bill was set aside at the end of July and may not be brought up again in its entirety this year, we want to explain here why we are concerned with Section 701 and why we believe it should be stricken from the bill (and not included in any free-standing legislation to encourage cybersecurity information sharing).

I. Cybersecurity "Countermeasures" – What Are They?

Our objections to Section 701 focus on the concept of "countermeasures" and stem mainly from what we don't know: We don't know exactly what limits in current law the "countermeasures" language is intended to overcome or what conduct it would authorize that is not already permitted.

We know that ISPs and other network operators already block spam and other malicious traffic,[1] and we support their right to do so. We also know that there is discussion about "active defense" that encompasses a wide range of responses to cybersecurity threats.[2] As far as we know, no one has publicly identified the problems in current law that the Senate countermeasures language is intended to address, and no one has publicly identified what countermeasures would be authorized that are now prohibited. It is not even clear that the Wiretap Act or the other electronic surveillance laws that Section 701 would trump inhibit such measures (whatever they are).

The bill's definitions do not really help. In Section 708(2) of the bill, "countermeasures" are defined as "automated or manual actions to modify, redirect, or block information that is stored on, processed by, or transiting an information system that is known or suspected to contain cybersecurity threat indicators for the purpose of protecting an information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected."

Under Section 708(7)(A)(viii), a "cybersecurity threat indicator" is defined to include "any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law." Under Section 708(6), "cybersecurity threat" is defined as "any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, process by, or transiting an information system... "

The drafters of the bill have tried to assure that the countermeasures that would be authorized cannot include discriminatory conduct that would violate the FCC's "net neutrality" rules. Section 707(10) says that nothing in Title VII of the Act may be construed "to authorize or limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet." (Those rules are being challenged in court; if they are set aside, it is unclear what, if any, discriminatory conduct might be permitted by Section 701.)

However, the immunity language of Section 706 goes beyond the authorization language of Section 701. While Section 701 "only" overrides specific provisions of federal law protecting the

[1] The FCC's open Internet rules expressly recognize and preserve the authority of service providers to address harmful traffic. "Examples include spam, botnets, and distributed denial of service attacks. Unwanted traffic includes worms, malware, and viruses that exploit end-user system vulnerabilities; denial of service attacks; and spam. FCC, Preserving the Open Internet: Final Rule, 76 Fed. Reg. 59191 (Sept. 23, 2011) at n. 102.

[2] Joseph Menn, "Hacked companies fight back with controversial steps," Reuters, June 17, 2012 http://www.reuters.com/assets/print?aid=USBRE85G07S20120617.

privacy of communications,[3] Section 706(b) provides that "a reasonable good faith reliance that this title permitted the conduct complained of is a complete defense against *any* civil or criminal action brought under this title or *any other law*." This might, for example, impact commercial disputes over quality of service guarantees. In an era of increasing reliance on the Internet for critical business services and increasing bandwidth demands, service providers and customers will be negotiating guaranteed service levels. Section 706(a), in covering all civil actions, would foreclose breach of contract actions. The Section 706(a) immunities are largely limited to information sharing and monitoring authorities, but the 706(b) good faith defense applies to any conduct "permitted by this title" and thus would seem to be available in contract actions brought for violation of quality of service obligations where the service provider claimed that its actions breaching the contract were undertaken for cybersecurity purposes.

For example, a provider of electronic communication service may promise to provide a client that relies heavily on video streaming a specified quality of service for video traffic, with guaranteed transfer rates and maximum packet loss and/or latency thresholds. Under the countermeasures authority granted in the bill, the provider could employ countermeasures that result in slower rates, more packet loss, or higher latency than agreed, thus breaching its quality of service contractual commitments and causing demonstrable damages to the client, who would be unable to provide the quality video streaming its customers depend upon. The client would have no recourse: if the statute authorized the countermeasures and the provider undertook them in good faith, the provider has a complete defense to a suit brought to enforce the contractual commitment to provide a specified quality of service.

Cybersecurity measures and countermeasures are likely to become more automated, for good reason. In this context, we believe that Internet access providers and their customers (including enterprise customers) deserve clearer guidance on what actions might be taken by service providers to interfere with Internet traffic.

II. Monitoring

CDT agrees that network operators should have the authority to monitor traffic in order to protect their own systems against cyberattacks (and we believe they have that authority under current law). This kind of monitoring, when done appropriately by companies, benefits Internet users. We recognize that there is doubt about whether ISPs and other network operators can monitor their networks in order to protect the broader ecosystem, for example, by monitoring for threats that are not directly affecting the particular provider or its customers.[4] CDT has

[3] Specifically, the "notwithstanding" language of 701 applies to the Wiretap Act (chapter 119 of Title 18), the Stored Communications Act (chapter 121 of Title 18), the pen/trap statute (chapter 206 of Title 18), the Foreign Intelligence Surveillance Act, and Sections 222 and 705 of the Communications Act (47 U.S.C. 222 and 605).

[4] 18 U.S.C. 2511(2)(a)(i) specifies that it is not unlawful for a provider of electronic communication service to intercept, use or disclose a communication while engaged in an activity which is a necessary incident to the protection of the rights or property of the provider of that service. This does not expressly allow the service provider to engage in monitoring to protect the users of its system (compare 18 U.S.C. 3121(b)(1)) or to protect other entities in the ecosystem.

suggested language that would narrowly address that problem.

We also understand that the "all party consent" rule of about a dozen states limits the ability of service providers to rely on the consent of their customers to monitor communications. Section 707(b) would address that concern by pre-empting state law.[5]

But, so far, there is no statement from the bill's drafters explaining what are the elements of current law that need to be overcome nor any statement explaining what monitoring would look like under the bill's provisions.[6] Such information is essential to crafting the provision and to ensuring that it is used as intended in the future.

Section 701 is not targeted at amending the provisions of existing law to permit monitoring that need to occur. It operates "notwithstanding" the privacy provisions in the electronic surveillance laws. Instead of targeted amendments to specific laws, Section 701 strives to be narrow by listing the types of information or activity that can be monitored for. This may be as effective as specifying the purposes for which providers may monitor. However, the language in Section 701 allowing companies to monitor for any "attribute" of a cyber threat goes a step too far, as it could be read to authorize companies to monitor for nearly everything. The section's limitation that such monitoring is permitted unless otherwise prohibited by law is just unclear.

Concerns have been raised about the monitoring language when read in conjunction with the immunity language of Section 706. Sections 701(a)(1) and 701(a)(3) say that an ISP may monitor information passing over its system, and may give consent for others to monitor information passing over its system. This authorization applies even if the information being monitored pertains to or belongs to a non-consenting party and even if the party whose information is being monitored extracted a contractual commitment from the ISP not to monitor. Under 706(a), no civil cause of action can lie for monitoring activities authorized under 701(a)(1) or (3) even if the civil action is based on a negotiated agreement between the two parties. Whether the ISP breached the contract in good faith or bad, intentionally or not, no action shall lie to enforce the contractual obligation to refrain from monitoring.

---

[5] We are not sure that the preemption of state law would be unnecessary if the language of 2511(2)(a)(i) were carefully amended to allow monitoring to protect one's customers and other providers and their customers. Certainly, it seems that whatever monitoring is already permitted under 2511(2)(a)(i) is not illegal in all party consent states. We assume that, if service providers were allowed to engage in cybersecurity monitoring to protect both their systems and the systems of others, no consent (not even the consent of one party) would be needed on top of that exception, and the all party consent laws would be irrelevant.

[6] The fullest public explanation we have seen of the problem is found in a recent report by the Bipartisan Policy Center. http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf. However, that reports notes that the judicial rulings that worry some companies are in older cases involving telephones. The BPC report does not specifically mention that one of the provisions specifically relied on by the courts in those older decisions – the statement in 2511(2)(a)(i) that limits random monitoring -- only applies to providers of wire (that is voice) communications and does not apply to ISPs or other operators of Internet services.

As does "good faith" liability protection for countermeasures, complete immunity for monitoring could upset contractual quality of service obligations. Building on the previous example, the promise by a provider of electronic communication service to give a client that relies heavily on video streaming a particular service quality, with guaranteed transfer rates and maximum packet loss and/or latency thresholds, may become unenforceable. Under the monitoring authority granted in the bill, the provider could engage in monitoring activities that slow transfer rates or increase packet loss or latency beyond what is permitted by contract, thus breaching its quality of service contractual commitments and causing losses to the client. The client would have no recourse: the monitoring was authorized by the statute; the ISP is given complete immunity for doing it; the client's suit to enforce the contractual commitment to provide a specified quality of service would be immediately dismissed.

As Paul Rozensweig of the Chertoff Group has concluded about a similar immunity provision for information sharing, "The way I read that it also includes an exemption from liability for the breach of contractual obligations. So if, say, your ISP promises you in a contract never to share any information with the Federal government and it then goes ahead and shares information with a cyber exchange, you can't even sue for actual damages."[7]

III. Conclusion

Companies already have substantial authority under federal law to intercept, use and disclose information in order to protect their own rights or property. They can also hire third parties to do this work for them. They also already have authority to apply countermeasures to block malicious traffic. While a limited expansion of such authority may be needed to enable companies to monitor communications and block some of them in order protect others, the overbroad approach taken in the monitoring and countermeasures section of the Lieberman-Collins bill is not the answer.

The best thing Congress could right now, if it acts on cybersecurity as the number of days left on the 2012 legislative calendar dwindles, is adopt the Franken/Paul amendment to strike the monitoring and countermeasures section from the bill and take up the issue next year with hearings that link concrete solutions to concrete problems.

In the meantime, the White House or another governmental entity should convene a multi-stakeholder process through which tech and telecom companies, privacy NGOs and other stakeholders could develop a better shared understanding, on the public record, as to exactly what provisions in current law are improperly tying the hands of network operators, and what limited exceptions to them may be needed. The process may result in ideas for targeted legislation on which lawmakers could later act.

** This analysis is one of a series of posts from CDT on the Cybersecurity Act, S. 3414, a bill co-sponsored by Senators Lieberman and Collins that may be considered on the Senate floor this fall. For further information, please contact James X. Dempsey or Gregory T. Nojeim at CDT, 202/637-9800.*

---

[7] http://www.lawfareblog.com/2012/07/the-puzzling-liability-limitations-of-the-lieberman-collins-bill/?utm_source=twitterfeed&utm_medium=twitter