CDT POLICY POST
Volume 10, Number 12, July 16, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) CDT Report Calls for Continued ICANN Reform in Light of Internet Governance DebateCDT has issued a report calling for reform of the Internet Corporation on Assigned Names and Numbers (ICANN) in light of the growing worldwide debate over Internet governance. The report argues that the vision on which ICANN was founded -- bottom-up, inclusive private-sector coordination of domain name and numbering functions -- remains the best way to manage those critical functions while preserving the democratic character of the Internet. But CDT also believes that ICANN is straying from this vision, and it must change if it is to survive.

The success of ICANN has taken on greater importance given the new focus on Internet governance surrounding the U.N.'s ongoing World Summit on the Information Society (WSIS). ICANN has naturally become a target in the Internet governance debate because of its role in managing key Internet assets, and because it looks to many like a regulatory body that might be a precedent for centralized control of the Internet.

CDT's report, "ICANN and Internet Governance: Getting Back to Basics," offers suggestions for ICANN's reform based on the limited role it was intended to fill. CDT's report calls on ICANN to --

- visibly refocus on its core mission and disavow broader regulatory activities;
- embrace bottom-up consensus as a cornerstone of its approach; and
- do more to make ICANN inclusive.

Unless ICANN commits to this approach, it risks being altered or supplanted by international efforts to link its

management of Internet naming and numbering with broader "Internet governance" goals like content regulation. Such a result could well threaten the revolutionary decentralized characteristics that have been the hallmark of the Internet's promise to promote free speech, civic discourse, and economic opportunity around the world.

CDT's report is now available online at http://www.cdt.org/dns/ The report is being released in the lead-up to ICANN's meeting in Kuala Lumpur next week. Significant issues at that meeting will include ICANN's interaction with the WSIS "Internet governance" initiative, the introduction of internationalized (foreign language) domain names, and ICANN's greatly expanded proposed budget for next year.

---

(2) ICANN Meeting in Kuala Lumpur With Attention to WSIS Governance Debate The second ICANN meeting of this year will be held in Kuala Lumpur, Malaysia July 19-23. Among the issues of importance at the meeting are ICANN's expanded 2004-2005 budget, and its relationship to the ongoing WSIS process.

ICANN's controversial proposed 2004-2005 budget projects an almost doubling of ICANN's 2003-2004 expenditures, and is expected to be a significant point of discussion in Kuala Lumpur. Critics of the budget say it signals an unwise expansion in ICANN's size and activities. Supporters say the funds are necessary to perform ICANN's limited, but important role efficiently and effectively. At the very least, the dramatic increase in ICANN's budget raise questions about the power to increase fees paid ultimately by those who register domain names, and about the size and scope of ICANN's activities.

Real or perceived expansions of ICANN's role are of particular importance because of ongoing discussions about larger issues of Internet governance. This governance debate is a central focus of preparations for the second phase of the World Summit on the Information Society, culminating in November 2005. Concerns among governments participating in WSIS have led to calls for greater centralized Internet governance, or even some kind of general purpose, intergovernmental Internet governance body.

Many who have called for centralization of Internet governance have pointed to ICANN as a precedent. In part, this is due to the misperception that ICANN is a broad regulatory body with broad powers, when in fact ICANN has a very narrow mandate and very limited power. ICANN's role in this governance debate will therefore be another important focus of the Kuala Lumpur meeting.

Change in ICANN is needed-but not by making it an intergovernmental body or broadening its power. Rather, ICANN must be focused on the design that gave it birth, in order to save that vision of decentralized, bottom up coordination.

- It would have a narrow mission focused on the coordination of certain domain name and addressing functions.
- It would adopt policies within that narrow scope by bottom-up consensus among affected parties.
- Its processes would be transparent, predictable, and open to wide, global participation.

These principles were embodied in the U.S. Department of Commerce's White Paper, and later endorsed in the International Forum on the White Paper. The White Paper itself stressed that the plan it was outlining

"applies only to management of Internet names and addresses and does not set out a system of Internet 'governance.'"

ICANN's power was supposed to be limited in two important ways. One was express limitation on the subjects of ICANN's authority. For example, ICANN is not supposed to condition issuance of a domain name (or a block of IP numbers) on policies regarding the content that is distributed via the domain name.

The second mechanism was consensus-based decision-making. Generic Top Level Domain (gTLD) registries (like .com or .org) are only bound to comply with policies from ICANN that reflect an actual, documented consensus among affected parties. This was designed to ensure that ICANN could not overreach by passing rules without the consent of those affected by those rules.

Instead, in many ways ICANN is departing from these mechanisms. CDT's report outlines how ICANN has used its "control" over the creation of new generic Top Level Domains (gTLDs) to force new registries and registrars to accept detailed controls on their operations. Even if today's ICANN Board disavows interest in overregulation, such overly detailed controls set a bad precedent-and communicate a potentially dangerous misimpression to the world-of ICANN exercising broader authority than many even within ICANN intend.

Moreover, the top-down impositions of obligations by ICANN's Board and staff have in many ways circumvented the bottom-up consensus approach on which ICANN was founded. The Independent Review Panel that was to serve as an appeals body has not, and may never be, created. And after abruptly eliminating the original structure that would have elected half of ICANN's directors to represent the Internet community at-large, ICANN has not yet developed adequate alternatives for public representation in its decision-making Ð sending a discouraging message to public interest groups and interested individuals.

---

(4) CDT Calls for Focus on Narrow Mission, Bottom-up Consensus Process Given the threats to private-sector coordination of naming and numbering posed by the Internet governance debates, CDT's report calls on ICANN to "get back to basics" through continued reform. Specific recommendations include:

- ICANN should recommit itself to the extremely limited mission it was created to accomplish. It should expressly disclaim governmental powers and reaffirm its limited focus in its bylaws and articles. Although some policy issues will be inextricably linked to ICANN's technical coordination role, it should minimize policy activities to the greatest extent possible.
- ICANN should adhere to the principle of subsidiarity and bottom-up decision-making-leaving decisions to local control unless there is a consensus that global policies are needed.
- Policy development should be transparent and predictable, with ICANN announcing proposals earlier and consistently following the processes it has established.
- ICANN should continue to pursue mutually acceptable relationships with the other key entities that manage critical Internet functions, like the root server operators, regional addressing registries, and country-code TLDs.
- ICANN should strengthen activities to engage diverse constituencies in its activities, reflecting the global diversity of Internet users.

Finally, both WSIS and ICANN need to allow the Internet to continue to develop as it has in the past, on the basis of global cooperation and bottom up, decentralized decision-making. That is the policy framework most likely to support growth of the Internet as an engine of freedom, economic empowerment and human development, particularly for developing nations.

CDT's report "ICANN and Internet Governance: Getting Back to Basics" is available online at: http://www.cdt.org/dns/icann/20040713_cdt.pdf

For more information about ICANN, domain names, or Internet governance more generally, please visit: http://www.cdt.org/dns/

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.12.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.12 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 13, July 30, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Email Privacy Protection Called into Question by Federal Appeals Court DecisionA recent court decision has revealed a significant gap in email privacy protection. The U.S. Court of Appeals for the First Circuit ruled in United States v. Councilman that an email provider does not violate federal wiretap laws when it opens emails to its customers and uses them for its own competitive business purposes. Although the decision applies only in a few New England states, its interpretation of Internet privacy laws if more broadly accepted would weaken protections for real-time communications over the Internet.

Current law provides different legal standards for access to communications while they are in transit and while they are in storage. Real-time access to communications in transit is subject to the strict procedures of the federal Wiretap Act (also called "Title III"). The Stored Communications Act provides less stringent standards for obtaining access to stored emails. Councilman essentially moved Internet communications from the more stringent requirements of Title III to the less stringent protection of the Stored Communications Act.

In Councilman, the email provider was copying customer emails on an ongoing basis just before they were placed into the recipients' mailboxes on the provider's server. The court found that because the email messages were very briefly stored (literally for milliseconds) on the ISP's computer before going into the recipients' mailboxes, the ISP did not violate the Wiretap Act's prohibition on intercepting email while it is in transit.

Since digital transmissions are stored in RAM or on hard drives at each step along their path while computers process them and send them on their way, all email could be accessed while in "storage," and most acquisitions of email would fall outside the strict rules of Title III. This has significant privacy ramifications with regard to both law enforcement and ISP access to Internet communications.

- United States v. Councilman
- The Wiretap Act ("Title III")
- The Stored Communications Act

---

(2) Loophole for Law Enforcement Access to Internet Communications The First Circuit's interpretation creates a potential loophole for law enforcement agents to intercept email or other Internet-based communications in real time without abiding by the strict requirements of Title III. Because ongoing interception of communications is uniquely intrusive, Title III prohibits real-time interception of voice or email communications in transit without a wiretap order and other procedural safeguards. The Councilman decision undermines that requirement. Instead, access to email that is essentially real-time would be subject to the lower standards of the Stored Communications Act, which sometimes require a search warrant for government access and sometimes permit government access with a mere subpoena - meaning there is no court approval at all.

With a search warrant or subpoena, the government is only supposed to get whatever the service provider has in storage at the time the order is executed. Even the Department of Justice has always assumed that ongoing access to Internet communications requires a wiretap order under Title III. The Councilman decision calls that interpretation into question.

---

(3) ISPs Can Access Email in Transit Without Violating Wiretap Act In addition to the question of government access, the Councilman decision has highlighted a weakness in the privacy duties of ISPs. Councilman did not change the law in this regard, but it pointed out that while email is in storage with an ISP, an ISP can read and use that email, without notice or consent, for its own business purposes. ISPs have legitimate reasons for reviewing email, such as protecting the security of their networks, but the law also allows an ISP to use a customer's email for its own purposes unrelated to providing Internet service and without notifying the customer.This is clearly inconsistent with the spirit and intent of the electronic privacy laws, clearly incompatible with the expectations of users, and clearly at odds with industry norms as reflected in the privacy policies of major ISPs. In the Electronic Communications Privacy Act of 1986, which amended Title III and created the Stored Communications Act, Congress intended to provide privacy protection to email that is roughly comparable to that afforded telephone calls and postal mail.

It is now clear that there is an unintended loophole in the law. ISPs should only be allowed to read and use their customers' email when necessary to protect the ISPs' rights or enforce the terms of service, or with prior informed consent. Councilman did not significantly change the rules for ISPs, but it highlighted a major loophole in our privacy laws, which essentially permit ISPs to access and use, and in some cases even disclose to others, their customers' stored email.

---

(4) Legislative Fixes Being Considered Congressional action to address both aspects of the Councilman decision has already begun. A bipartisan group of Members of Congress introduced a House bill, the E-mail Privacy Act of 2004 (H.R. 4956), which would amend both Title III and the Stored Communications Act. The

bill, sponsored by Rep. Jay Inslee (D-WA) and cosponsored by Rep. Jeff Flake (R-AZ), Rep. Roscoe Bartlett (R-MD), and Rep. William Delahunt (D-MA), would both ensure that law enforcement officials have to obtain a wiretap order in order to engage in real-time acquisition of Internet communications, and that ISPs cannot read and use their customers' email except where necessary to provide service or with consent. A second bill, H.R. 4977, sponsored by Rep. Jerrold Nadler (D-NY), addresses the same issues.

- H.R. 4956
- H.R. 4977
- More on wiretap laws

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.13.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.13 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 14, September 10, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Federal Court Strikes Down Pennsylvania Law That Blocks Innocent Web Sites On September 10, 2004, Judge Jan DuBois of the U.S. District Court for the Eastern District of Pennsylvania invalidated Pennsylvania's "Internet Child Pornography" law, finding that the law has blocked access to more than one million wholly innocent web sites, while having little if any effect on the few hundred child pornography sites that were targeted by the law. In one instance described by Judge DuBois, access to the web site of a rural Pennsylvania community recreation center was blocked as a result of a blocking order issued to an Internet Service Provider (ISP) by the Pennsylvania Attorney General. The blocking order targeted a single child pornography site, but resulted in the blocking of thousands of innocent web sites.

The Pennsylvania law imposed potential criminal liability on ISPs for child pornography available on the Internet, even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content. The law makes any ISP doing business in Pennsylvania potentially liable for content anywhere on the Internet.

The court declared that the Pennsylvania statute violated the First Amendment and the Commerce Clause of the United States Constitution. The law was passed in 2002 by the Pennsylvania legislature without any investigation into how the law would impact Internet communications.

---

(2) Court Decision Issued in Legal Challenge Filed by CDT, ACLU On September 9, 2003, CDT together

with the ACLU of Pennsylvania and Plantagenet, Inc., a Pennsylvania ISP, filed a constitutional challenge to the Pennsylvania statute. The challenge argued that the Pennsylvania law was a prior restraint on speech that violates the First and Fourteenth Amendments and the Commerce Clause of the Constitution.

The law provided that the state Attorney General or any county district attorney can unilaterally apply to a local judge for an order declaring that certain Internet content may be child pornography, and requiring any ISP serving Pennsylvania citizens to block the content. The entire court proceeding occurred with only government participation and no prior notice to the ISP or the web site owner, violating the First Amendment's protection against prior restraints. As court testimony established, the technical design of the Internet dictates that most ISPs can only comply with the blocking orders by also blocking a significant amount of wholly innocent web site content as well.

The Pennsylvania Attorney General went further, bypassing the law's inadequate court procedures by simply issuing secret orders to ISPs to block content. During 2002 and 2003, the Attorney General secretly issued, without court approval or opportunity for appeal, almost 500 blocking orders directed at about 400 Internet web sites that the AG asserted contained child pornography. The blocking orders had the effect of blocking access to more than one million innocent web pages that had no relationship with child pornography.

On the day CDT and the ACLU filed the lawsuit, the Attorney General agreed to halt his secret censorship orders, and the court entered an injunction against those orders. That injunction was reaffirmed by the court decision striking down the entire statute.

---

(3) Pennsylvania Child Pornography Statute Raised Legal and Technical Problems The Pennsylvania law raised very serious problems - both legal and technical. The law violated constitutional principles of free speech and due process. Compliance with the law also resulted in the blocking of web sites completely unrelated to any child pornography sites also be blocked, simply because most Internet web sites today share their "Internet Protocol" (or "IP") addresses with many other wholly unrelated web sites.

Expert testimony presented by CDT evaluated the magnitude of over-blocking. That testimony demonstrated that more than two-thirds of all .COM, .NET, and .ORG web sites share their IP addresses with at least fifty other web sites. Any blocking order aimed at one of those web sites under the Pennsylvania law also blocked all fifty (or more) sites, even if those sites are wholly unrelated to the targeted web site. In some cases presented to the court, the IP address of a child pornography site was shared by more than 400,000 other web sites, and all 400,000 sites were blocked.

In addition, the law also forces ISPs to manipulate the sensitive "routing tables" used to send communications around the Internet, increasing the risk of major Internet service outages.

Information about the lawsuit is available at http://www.cdt.org/speech/pennwebblock/, and key litigation documents and expert reports are at http://www.cdt.org/speech/pennwebblock/penndocs.shtml.

---

(4) Child Pornography Deserves More Effective and Focused Law Enforcement EffortsCDT shares the belief that child pornography has no place in any civilized society, and supports the vigorous prosecution of those responsible for the creation of such material.

The Pennsylvania statute struck down by the court's decision, however, did very little to remove the child

pornography at its source or to prosecute those who create and post the content. Evidence presented to the court established that the Pennsylvania statute had little if any impact on people interested in accessing child pornography, while at the same time having massive impact on wholly innocent web sites.

There is a wide range of less constitutionally damaging but more effective alternatives available to government to combat child pornography, including working with national and international investigators, including the Federal Bureau of Investigation and the U.S. Customs Service, to investigate and prosecute the creators and knowing distributors of child pornography. With the proper procedural protections, law enforcement could also directly contact the web host (or hosting ISP) about the alleged child pornography to seek to have the content removed at the source.

In contrast to those approaches that directly target the child pornography and its makers, the approach used in Pennsylvania actually allows the child pornography to continue to circulate on the Internet. Under the law struck down by the court, Pennsylvania took no action against the makers or distributors of child pornography.

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.14.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.14 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 15, September 29, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

Please note that CDT reissues Policy Post Volume 10, Number 15 to correct inaccuracies related to our description of the Sender Policy Framework. CDT regrets the error and apologizes for any inconvenience.

---

(1) Spam Continues to Plague Industry and Users

As of June 2004, approximately 60% of all email was spam. Measures such as the federal CAN-SPAM Act, which took effect in January 2004, have had limited impact. Certainly, nothing has yet turned the tide. If anything, spam appears to have become more invasive: spammers distribute viruses, spyware, and surreptitious spamware. "Phishing" capitalizes on spam to perpetrate fraud against online consumers.

In July 2004, CDT convened a meeting of industry, consumer advocates, human rights campaigners, and technologists to discuss the status of anti-spam efforts. As the CAN-SPAM Act had gone into effect six months earlier, mid-summer was an opportune time to evaluate the extent to which Internet users were experiencing some relief from spam, and to examine the responses of law enforcement, industry and technology developers.

The concerns of ISPs focus on the costs spam imposes, costs that end-user filtering does not address. Mainstream companies doing business online worry about the efficacy of email as a communications medium. Increasingly, they are concerned about whether legitimate email -- for example, purchase confirmations -- will get through. Some progress has been made in developing good practices for email marketing, such as committing to solely permission-based marketing lists. Strategies of email marketing may be moving away from acquisition of email lists and toward retention of existing customers.

Consumers are frustrated with the lack of reduction in the incidence of spam since the passage of the CAN-SPAM Act. Consumer advocates point to the fact that users have no private right of action against spammers under the Act. Businesses respond that an industry-sponsored consumer education program could focus on consumers' online behaviors that result in their receipt of spam.

Both consumer advocates and businesses note that providing the means to identify and authenticate senders is key to resolving the spam problem. However, issues of protection of legitimate anonymity remain to be resolved.

A report summarizing the July discussion and highlighting areas of agreement, disagreement, and ongoing concern is available at http://www.cdt.org/speech/spam/20040715consultation.shtml.

For CDT's analysis of the CAN-SPAM Act at the time it was enacted, see http://www.cdt.org/speech/spam/031211cdt.pdf

CDT's analysis of why consumers receive spam and what they can do to curtail it is at http://www.cdt.org/speech/spam/030319spamreport.shtml

---

(2) Enforcement Efforts Increase, But Face Challenges Pursuant to the enforcement provisions of the CAN-SPAM Act, several states have brought cases against spammers under the law. At the federal level, at least 62 cases have been brought by the Federal Trade Commission. Most of the cases brought against spammers were based on allegations of deceptive trade practices.

Identifying spammers is a key challenge to efforts to enforce spam laws. Another is the lack of enforcement agents with the necessary experience, training and skills. In many states, the attorney general's office lacks the resources to train staff to adequately enforce spam laws.

ISPs have also begun to bring enforcement actions, and the industry says that the level of resources employed in fighting spam and the skill of personnel working on the cases have increased.

---

(3) Technology Proposals Are Seen as Key Given the limitations of enforcement, attention is turning to technological solutions. Proposals focus on key characteristics of email and email senders - reputation and identity; adherence to best practices; and filtering by the end user.

The Sender Policy Framework (SPF) contemplates an infrastructure that relies upon identity and evidence to assure that a sender is who he says he is; prevention agents that detect denial of service attacks, assess sender reputation and filter outbound messages; and protection filters that prevent spam from reaching the end user's inbox. SPF is a technical standard that works in conjunction with a program that includes government-industry partnerships, strong spam laws, interagency cooperation in enforcement efforts; industry standards and policies; and educational programs to inform users about tools and best practices for dealing with spam, as well as about how to assure the deliverability of their own messages.

The TRUSTe-Bonded Sender program identifies and authenticates legitimate email. The program identifies senders who are pre-qualified through the Ironport service. Once certified, the sender must post a bond for a specified amount, based on anticipated email volume. The Bonded Sender program debits the bond amount based on customer complaints. Once certified, Bonded Sender places the sender on its whitelist. If there is a

sudden rash of complaints or other significant cause for concern about the sender's behavior, the sender is temporarily suspended. Bonded Sender employs a business-to-business dispute resolution process.

Habeas promotes sender best practices, provides feedback about senders, and ensures deliverability of messages. The goal of the Habeas solution is to help senders establish identification and authentication practices. Habeas uses a complaint resolution process that currently investigates every complaint received by the company.

For more information:
TRUSTe-Bonded Sender program: http://www.bondedsender.com/
SPF: http://spf.pobox.com
Ironport: http://www.ironport.com/
Habeas: http://www.habeas.com/

---

(4) Technical Solutions May Implicate Non-Profits and Political Speech Anti-spam technical solutions, especially those implemented at the ISP level, raise issues non-governmental organizations. Several issues warrant further consideration, including:

- The risk that legitimate messages sent by NGOs will be falsely identified as spam and blocked, without notice to the sender.
- Retention of end users' control over their inboxes.
- The need to preserve anonymity for political speech in anti-spam solutions.
- The need for political speakers to be able to respond quickly by email, without getting permission from a bonding agent.
- Due process for all parties in resolving complaints and disputes related to spam. Those complaining about spam should be held accountable that their claims are legitimate, so that political speech and unpopular speech are not blocked in a discriminatory way.

CDT expects to continue its examination of the spam issue with a follow-up meeting focusing on these free expression issues.

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.15.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.15 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 16, October 4, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Senate Amendments Propose PATRIOT 2, Threaten Civil Liberties Today, the U.S. Senate begins voting on amendments to legislation to reform the intelligence agencies. Two amendments in particular threaten civil liberties. Both are sponsored by Sen. Jon Kyl (R-AZ).

The Senate intelligence reform legislation would create a Civil Liberties Board in the Executive Branch of the federal government to oversee counter-terrorism programs that have implications for privacy or free speech. The Senate bill also would create Privacy and Civil Liberties Officers in various federal agencies that handle personal information. Together, these two mechanisms could provide important checks on government overreaching.

One of Senator Kyl's amendments would weaken the proposed Civil Liberties Board and would remove the provision creating Privacy and Civil Liberties Officers. The amendment goes against one of the key recommendations of the 9/11 Commission, which is that we need a cross-agency oversight board to protect privacy and civil liberties in an age of greater information sharing and powerful new technologies. CDT believes that the provisions under attack by Sen. Kyl must be part of any legislation to implement the 9/11 Commission's report.

- CDT Letter Opposing the Kyl Amendment to Gut the Civil Liberties Board: http://www.cdt.org/security/patriot2/20041001cdt.pdf

Sen. Kyl (R-AZ) has also introduced an amendment to the Senate bill that would expand the USA PATRIOT Act with a variety of new powers, including giving the FBI so-called "administrative subpoena" authority, meaning that FBI agents could demand paper and electronic documents without judicial approval. A broad coalition of public interest groups from across the political spectrum is opposing the Kyl PATRIOT 2

amendment.

- Right-Left Coalition Letter Opposing Kyl "Patriot 2" Amendment: http://www.cdt.org/security/patriot2/20041001coalition.pdf

---

(2) Background: 9/11 Commission Legislation Has Serious Implications for Privacy and Civil Liberties
Under the pressure of election year politics, both the House and Senate are considering legislation to reform the nation's intelligence agencies. In the process, privacy and other civil liberties are at risk.

The legislation is intended more or less to implement the recommendations of the commission that studied the intelligence failures associated with the 9/11 attacks. The bipartisan commission issued its best-selling report on July 22, 2004. Immediately, some politicians called for swift adoption of the Commission's recommendations, which include the establishment of a National Intelligence Director and the creation of a government-wide information sharing capability.

The Senate bill has been reported by Committee and is pending on the Senate floor, to be voted on this week. The House will take up its bill on Wednesday, October 6. The Senate bill addresses only issues raised by the 9/11 Commission, but the House bill extends far beyond the scope of the Commission's report.

- 9/11 Commission Report: http://www.9-11commission.gov/report/index.htm
- Senate Bill, S. 2845 http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02845:
- House Bill, H.R. 10 http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.00010:

---

(3) What Should -- and Should Not -- Be Part of the Intelligence Reform Legislation The legislation to implement the recommendations of the 9/11 Commission should do just that - and no more. Yet the House bill contains many controversial provisions that are well outside the scope of the Commission's report. Among the far-reaching proposals in the House bill that were not recommended by the 9/11 Commission is the creation of a de facto national identification card based on requiring states to link together all of their drivers license databases. While CDT has long argued that identification documents need to be made more secure, we should not - and need not - create a national ID card.

The House bill does contain a provision creating Privacy and Civil Liberties Officers, but it does not include the Civil Liberties Board that can look at issues that cut across agencies, such as information sharing and watch lists. Lacking from both bill at this point is a clear prohibition against the CIA and defense intelligence agencies engaging in covert operations in the United States.

Information sharing is an important issue that CDT believes is unquestionably an important part of intelligence reform. The Senate bill is intended to promote information sharing and bring it within a framework of transparency, guidelines and accountability. CDT believes that the Senate language should be maintained and clarified to make it clear that the system could be used only for counter-terrorism purposes and that major implementation will not occur until after Congress has had a chance to review the Administration's plan and privacy guidelines.

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.16.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.16 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 17, October 12, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) FTC Files First Spyware Case, Based on CDT Complaint The Federal Trade Commission (FTC) filed suit in the District Court of New Hampshire on October 7 against Seismic Entertainment and a former self-styled "Spam King," Sanford Wallace, taking up a complaint filed by CDT last February. Although the FTC has formerly brought cases against "dialers" and online "mouse trapping" schemes designed to keep users from closing web sites, the current case is widely considered to be the first major suit by the FTC in the core area of spyware.

CDT's complaint alleged that Seismic engaged in browser hijacking and deceptive advertising. Following in-depth research, CDT concluded that Seismic purchased banner ads that ran on web sites related to gaming, sports, and other topics. The ads often appeared as public service advertisements, but when loaded they would change a user's homepage and trigger a stream of pop-ups, including misleading advertisements for "Spy Wiper" or "Spy Deleter" anti-spyware software. CDT also subsequently showed that a Seismic website caused forced installations of advertising software and other programs.

The FTC's suit against Seismic and Wallace, its owner, mentions these and other actions as violations of the FTC Act. The FTC alleges that "in numerous instances, Defendants' practices cause or have caused consumers' computers to malfunction, slow down, crash, or cease working properly, and cause or have caused consumers to lose data stored on their computers."

- FTC Press Release Announcing Case against Seismic, Smartbot.net and Sanford Wallace, October 12, 2004 http://www.ftc.gov/opa/2004/10/spyware.htm
- FTC Complaint in the US District Court in New Hampshire http://www.ftc.gov/os/caselist/0423142/0423142.htm

- CDT's complaint to the FTC against MailWiper and Seismic Entertainment Productions [PDF], February 10, 2004 http://www.cdt.org/privacy/20040210cdt.pdf

---

(2) FTC Case Sets Valuable Precedent For Better Enforcement Since CDT's initial report on the spyware issue in November 2003, we have argued that existing statutes cover many spyware practices. Relevant laws include the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the FTC Act prohibiting unfair and deceptive business practices.

The dearth of enforcement of these laws in the spyware context has been partially responsible for allowing spyware to flourish online. At a House hearing in April, Rep. Joe Barton, Chairman of the House Commerce Committee, criticized the FTC for failing to bring any spyware cases. The FTC's current action therefore represents an important step toward better enforcement against spyware purveyors.

A recent Consumer Reports survey found that over a third of home Internet users have had their homepage hijacked. The proliferation of deceptive advertising for anti-spyware products is also a prevalent problem. The FTC's current case squarely targets these practices, and lays the groundwork for future spyware cases in other areas.

CDT plans to continue bringing cases to the FTC. CDT encourages users that have been hit by spyware to submit their stories to http://www.cdt.org/action/spyware. CDT reviews and researches reports and will file complaints where appropriate.

---

(3) House Passes Two Spyware Bills, Leveling Civil, Criminal Penalties Congress pushed forward on the spyware issue, as the House approved two separate anti-spyware bills.

H.R. 2929, known as the "SPY ACT," was passed on October 5th. It would create civil penalties for certain deceptive practices related to spyware. The list of targeted practices is based on a consensus document produced by the Consumer Software Working Group, which CDT convened last spring. A broad range of industry and consumer groups endorsed that list, and have worked with the Committee to refine this section of H.R. 2929.

The SPY ACT would also require that consumers be given notices prior to the execution of adware and other software that transmits personal information. CDT and other groups raised concerns that this section was poorly targeted in earlier versions of the legislation. Recent amendments have sought to focus the notice requirements and eliminate the need for redundant notices.

The second bill, H.R. 4661, known as the "I-SPY Act," would establish criminal penalties for those who use spyware to steal personal information or to commit other federal crimes. This bill, passed by the House on October 6th, would create high penalties for the most egregious types of spyware.

While CDT still believes that privacy legislation addressing the full range of online privacy concerns is needed and would address many of the issues implicated by spyware, the current bills would be a helpful initial step toward combating the problem.

- Text of HR 2929, Securely Protect Yourself Against Cyber Trespass Act

http://www.cdt.org/privacy/spyware/20040924cdtcommerce.pdf

- Text of HR 4661, Internet Spyware Prevention Act http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4661:
- CDT's Testimony before the House Subcommittee on Commerce, Trade, and Consumer Protection on H.R. 2929 [PDF] , April 29, 2004 http://www.cdt.org/testimony/20040429schwartz.pdf

---

(4) Senate and House Seek to Reconcile Approaches In Time for November Session In contrast to the House, the Senate has yet to pass a spyware bill. S. 2517, the "SPY BLOCK" Act, was approved by the Senate Commerce Committee in September, and awaits consideration by the full Senate. The bill includes the criminal provisions of the House criminal bill, and prohibits a list of deceptive practices similar to that in the House civil-penalties bill.

The biggest difference between the House and Senate bills is in their requirements for notice on installation of software. The Senate bill prohibits deceptive installations, but does not include the level of detail in mandating the wording of notices that is present in its House counterpart. CDT prefers the Senate's approach, which we believe will provide needed flexibility for different kinds of devices and interfaces.

Although the House and Senate are now in recess, both are expected to meet again briefly in a "lame duck" session in November. House and Senate staff are working to reconcile the three bills in order to have them ready for this session.

Meanwhile, states continue to push forward with their own laws. California Governor Arnold Schwarzenegger signed a spyware bill on September 28, prohibiting several deceptive spyware related practices in California. This makes California the second state, after Utah, to pass specific anti-spyware legislation.

- Text of S. 2145, "SPY BLOCK" Act http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.02145:
- Text of California SB 1436 http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4661:
- CDT Testimony before the Senate Commerce Committee on S. 2145 http://www.cdt.org/testimony/20040323berman.shtml

---

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.17.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.17 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 18, October 14, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Intel Reform Bills Threatening Civil Liberties on Fast Track House and Senate staff are meeting to resolve differences between competing versions of intelligence reform legislation intended to implement recommendations of the 9/11 Commission. While press reports have stressed differences between the bills, compromise is likely within the next week. Important civil liberties issues are at stake.

The House bill, drafted in a highly partisan atmosphere, is of special concern. The bill contains a few privacy-enhancing provisions, but is weighted down with PATRIOT 2 expansions of government discretion, harsh immigration-related provisions, the outlines of a national ID card, and a welter of "information sharing" mandates and systems without a coherent plan or civil liberties guidelines.

CDT is urging members of Congress to adopt the Senate version of the bill, but to reconsider that bill's provisions on ID cards and checkpoint screening.

---

(2) Senate Information Sharing Provisions Include Privacy Requirements and Oversight Both bills attempt to address one of the major problems in US counter-terrorism efforts: the failure of government agencies to share information and "connect the dots."

The Senate bill is far preferable. It takes a comprehensive approach, requiring the Executive Branch to first develop a system design and privacy guidelines for information sharing. Section 206 of the Senate bill calls not for centralization of data but rather for --

- a set of pointers and directories to information, which can be shared only with appropriate authorization;
- adoption of policy and privacy guidance before any system is built;
- a requirement on the front end of a system design plan weighing costs and impacts;
- phased implementation to allow Congressional and public reaction; and
- a strong civil liberties board to oversee and ensure privacy safeguards.

The Senate bill requires the Administration to submit its system plan and the privacy guidelines to Congress before major implementation can go forward. After the plan and guidelines are submitted, Congress can (and should) hold hearings. Congress can rewrite the guidelines if they are inadequate. The normal appropriations process will have to be followed.

While the Senate proposal is based on accountability, privacy guidelines, and Congressional oversight, the House bill offers an incoherent amalgam of information sharing provisions without privacy guidelines or other safeguards. Sections 2192 and 3101 of the House bill should be deleted in lieu of § 206 of the Senate bill.

The House bill also includes other information collection and sharing initiatives without adequate privacy safeguards or redress, including § 3081, which requires a study on creating a lifetime travel history database on American citizens, and §§ 2142 and 2144, which expand private employer access to FBI criminal history records.

Both bills include provisions that would increase reliance on the driver's license as a de facto national ID card. The Senate bill includes language added at the last minute promoting more ID checks at screening points. These are complex and difficult issues that cannot be safely resolved under the time pressure of an election year. Therefore, CDT believes that ID card and screening provisions of both bills should be reconsidered.

- CDT Statement on Civil Liberties and Information Sharing, Oct. 4, 2004

- Enhancing Security and Civil Liberties -- An open letter from Dave Farber, Esther Dyson and Tara Lemmey, Oct. 6, 2004

---

(3) New Intelligence Agency Raises Concerns Both bills call for the creation of a National Intelligence Director (NID) to coordinate Intelligence reform. Coordination is certainly needed, but both bills lack clarity on a few key questions:

- Neither bill imposes limits on CIA and Pentagon domestic covert operations. This should be fixed.

- The National Intelligence Director appears to have authority to "task" the FBI. It should be made clear that this does not allow the NID to direct domestic surveillance outside the normal constraints to which the FBI is subject.

- The House bill includes a new definition of national intelligence that includes any and all domestically gathered intelligence and purely domestic threats. The Senate version is much narrower and should be

adopted.

---

(4) House Bill Laden with PATRIOT 2 Provisions The House bill contains a number of provisions from the Justice Department's never-introduced PATRIOT 2 legislation, expanding government powers, infringing on privacy, and limiting due process. While many of these do not relate to the Internet or other communications technologies, CDT believes it is a perversion of the process to include them in legislation intended to reform the intelligence agencies. Once again, a genuinely urgent issue - the need to reform the intelligence agencies - is being used for unrelated expansions of government discretion.

Here are the PATRIOT 2 provisions, which CDT is urging Senators to reject:

- § 2001 - extension of secret domestic intelligence surveillance to individuals without proven connection to a foreign terrorist organization or foreign government (FISA "lone wolf");
- § 2043 material support - expansion to cover mere membership in an organization;
- §§ 2602-2603 - expansion of preventive detention and lifetime supervision;
- §§ 2501-2503 - expansion of death penalty;
- § 4051 - expanded discretion to designate foreign groups as terrorist organizations;
- § 2191 - grand jury information - sharing grand jury information with foreign governments without adequate safeguards;
- § 3010 - suspension of habeas corpus in immigration cases.

The House bill also contains a number of immigration provisions going beyond the scope of the 9/11 Commission Report, which should be deleted: §§ 3006-3010, 3031-3035, 3052.

---

(5) Both Bills Contain Positive Provisions on Privacy Both the House and the Senate bills contain provisions that could enhance privacy protection. We would like to see all of these provisions included in the final bill, but if we had to choose one bill over the other, we would chose the Senate bill.

Here are the good privacy provisions in the Senate bill that should be retained (references are to sections of bill as passed out of Government Affairs Committee):

- § 211 - creating a strong privacy and civil liberties oversight board;
- §§ 126-127 and 212 - creating privacy and civil liberties officers in federal agencies involved in intelligence or law enforcement activities;

- § 206 - requiring privacy guidelines before information sharing can go forward;
- § 141 - establishing an Inspector General for the office of the new National Intelligence Director.

Here are the good privacy/civil liberties provisions in House bill:

- § 2173 - requiring no-fly/selectee list guidelines and a report by the Government Accountability Office (GAO);
- § 5091 - the Federal Agency Privacy Protection Act (FAPPA) - requires federal agencies to perform Privacy Impact Assessments on proposed federal rules that entail collection of personally-identifiable information
- § 5092 - establishes Chief Privacy Officers at agencies involved in law enforcement or counter-terrorism, similar to §212 of the Senate bill.

More Information:

- CDT testimony in support of privacy officers, Feb. 10, 2004
- CDT testimony in support of the Federal Agency Privacy Protection Act (formerly the Defense of Privacy Act), July 22, 2003

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.18.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.18 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 19, October 26, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Senate Holds Off on Copyright Inducement Bill, Further Efforts to Target P2P Likely

In recent weeks, there has been a flurry of activity In Washington on copyright legislation, focused mainly on the "Inducing Infringement of Copyright Act," S. 2560. The bill, formerly known as the INDUCE Act, was designed to target companies - especially makers of P2P file sharing software - that "induce" widespread copyright infringement .

Consumer groups and technology companies warned that, unless narrowly drafted, the law would impact a wide array of valuable consumer technologies. Intensive discussions among a range of interested parties, including CDT, failed to yield consensus language and the Senate Judiciary Committee put off a scheduled mark-up on the bill.

Although Congress will return after the election for a "lame duck" session, it is very unlikely that differences over the bill will be resolved this year. However, the issue will surely be back on the Congressional agenda next year, and it is likely that there will be further efforts to draft legislation. The sponsors of the Inducing Infringement of Copyright Act have said they remain committed to finding a way to hold accountable those who intentionally induce copyright infringement.

CDT has reiterated its willingness to work with others to try to find a balanced solution. CDT continues to emphasize, however, that any law must be narrowly tailored and cannot do collateral damage to innovation or basic technologies online. Thus, the impact of any bill on valuable and rapidly changing Internet technologies must remain a crucial benchmark.

- CDT letter, urging Senate Judiciary Committee to Hold Off Consideration of Inducement bill

- CDT's Copyright page

---

(2) Though Intended Narrowly, Inducement Drafts Would Have Swept in Valuable Technology Senators Orrin Hatch and Patrick Leahy, the sponsors of S. 2560, had stated that they sought a "technology-neutral law directed at a small set of bad actors while protecting our legitimate technology industries from frivolous litigation." CDT has voiced its support for this goal.

The latest drafts of S. 2560, emerging from intensive discussions in recent weeks, attempted to meet the goal by outlawing the manufacture of "peer-to-peer products" used for "viral distribution" where such infringement was "the principle reason the majority of users are attracted" to the product.

However, CDT and others pointed out that the proposed definitions would have swept in a broad range of legitimate consumer technologies, including products like TiVo, online collaboration tools, new instant messaging systems, and even web browsers. The bill would have created liability simply for manufacturing or selling such products if they became widely misused. This would have gone against the longstanding "Sony-Betamax doctrine," which assures product manufacturers that they cannot be liable for selling a product that has significant non-infringing uses.

The proposal of the Inducing Infringement of Copyright Act generated widespread grassroots response in the form of online activism and direct calls to Senate offices. This response was crucial to spreading understanding about the potential harmful impacts of the bill.

Senator Hatch, who is the chairman of the Judiciary Committee, acknowledged some of the concerns raised by current drafts of the bill as reasons for holding off consideration by the Committee for now.

Internet users should remain watchful and be prepared to engage their representatives again as future drafts are proposed.

---

(3) Other Copyright Measures Still Pending in Congress, Could Pass In addition to S. 2560, a variety of copyright enforcement measures mayyet come to a vote this year. These have been combined into a singlelong bill, H.R. 2391. The bill includes:

- A provision to criminalize the use of video recorders to tapepresentations of movies in theaters.
- A new copyright law education program, to be run by the Department ofJustice (DOJ);
- A voluntary program for ISPs, under which the DOJ would send ISPsnotices that particular subscribers are suspected of violatingcopyright law. The ISP would forward these warnings to theirsubscribers, without disclosing to the DOJ or third parties informationidentifying the suspected infringer.
- A measure to exempt the makers of devices that skip predeterminedparts of movies or other video content from any copyright liability.The provision was drafted to protect makers of "Clearplay" DVD playersand similar devices that automatically skip violence or otherobjectionable content in movies.

Devices that automatically skip

- A provision to allow the Department of Justice to bring civilcopyright cases, like those currently being brought by the RIAA againstpeer-to-peer users. Currently only private parties can bring civilcases, and consequently they bear the cost of such enforcement.

- A provision to lower the standard required for criminal copyrightprosecutions, aimed at users of peer-to-peer networks. The provisionwould change the required level of intent from "willfulness" to"reckless disregard" and would make it a federal crime to makeavailable even a single pre-release copyrighted work.

- This final provision lowering the bar for criminal copyright liabilityis one of the most controversial element of the bill. Critics have argued thatthe lowered standards could inappropriately turn what were formerlymuch smaller violations into federal felonies, and that such a sweepinglaw would invite selective enforcement.

Opposition to this and other elements of the bill prevented its passagebefore Congress adjourned at the end of October. The future of the billis uncertain. Sponsors are now working to answer some of theseobjections and hope to achieve passage when the lame duck Congressmeets in November.

More Information:

- Text of H.R. 2391

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.19.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.19 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 20, November 10, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Industry and Public Interest Groups Oppose Wiretap Design Mandates for the Internet

On November 8, 2004, CDT filed detailed comments on behalf of a diverse group of companies, trade associations and public interest groups from across the political spectrum opposing the plan of the Federal Communications Commission (FCC) to extend controversial wiretap design mandates to the Internet.

In a Notice of Proposed Rulemaking (NPRM) issued in August, the FCC proposed to declare that providers of broadband access and "Voice over IP" (VoIP) services are covered by the Communications Assistance for Law Enforcement Act of 1994 (CALEA). The FCC issued its NPRM in response to a petition filed by the FBI seeking to extend CALEA to broadband Internet access and services and to impose a government approval process before new Internet applications can be deployed.

Joint Comments of Industry and Public Interest, November 8, 2004
http://www.cdt.org/digi_tele/20041108intpubint.pdf

FCC Notice of Proposed Rulemaking, adopted August 4, 2004 (published September 23, 2004)
http://www.cdt.org/digi_tele/20040923nprm.pdf

---

(2) Background on CALEA and FCC's Proposed Extension of CALEA to the Internet The Communications Assistance for Law Enforcement Act (CALEA) was adopted in 1994 in response to law enforcement concerns that wiretaps would be more difficult in digital telephone networks than they had been in the analog phone system. CALEA required "telecommunications carriers," meaning telephone companies, to design basic wiretap capabilities into their networks. As it was implemented, CALEA gave the FBI very precise design control over telephone switches. The FBI was able to convince the FCC to mandate very specific features, including - at substantial cost to carriers - features that gave the government capabilities going beyond those that had been available in older phone systems. Thus CALEA was used to enhance rather than merely preserve government surveillance capabilities.

The CALEA statute applies only to telecommunications common carriers, and it specifically does not apply to "information services," meaning Internet applications. Congress realized in 1994 that the Internet was fundamentally different from the telephone system, and Congress chose not to apply CALEA to the Internet and "information services" carried over it. E-mail, Instant Messaging, VoIP, and other forms of Internet communications are information services and thus are not supposed to be covered by CALEA. Although ISPs and Internet application providers must (and do) comply with interception orders under the wiretap laws, they have not had to design their networks and services to meet FBI specifications.

In March 2004, the FBI filed a petition with the FCC asking that the agency extend CALEA to the Internet and to VoIP services over the Internet. The FBI also asked the FCC to create a pre-review process under which all new Internet applications and services would be screened by the FBI prior to deployment to ensure that they satisfied FBI criteria.

CDT and many others vigorously opposed the FBI's petition to the FCC. CDT filed comments and reply comments opposing the petition, and also organized a "joint statement" on behalf of a broad cross section of industry and public interest organizations detailing objections to the FBI proposal.

The FCC rejected the concerns of CDT and others and issued a Notice of Proposed Rulemaking announcing its tentative decision to extend CALEA to the broadband Internet and to certain VoIP services. The FCC decided that Internet access was a "substantial replacement" for local telephone service and that the CALEA statute therefore gave the FCC the power to extend CALEA to the Internet. The FCC rejected the FBI's request for a pre-approval process for new Internet services, but the ambiguous manner in which the FCC extended CALEA will have a similar harmful impact on innovation and the deployment of new technology on the Internet.

- Joint Statement of Industry and Public Interest, April 27, 2004 http://www.cdt.org/digi_tele/20040427jointcaleareply.pdf
- CDT Reply Comments, April 27, 2004 http://www.cdt.org/digi_tele/20040427cdtcaleareply.pdf
- CDT Comments to FCC on CALEA Petition for Rulemaking, April 12, 2004 http://www.cdt.org/digi_tele/20040412cdtcalea_comments.pdf
- FBI Petition to FCC for CALEA Rulemaking, Mar. 10, 2004 http://www.cdt.org/digi_tele/20040310fbipetition.pdf

---

(3) There is No Legal or Factual Basis for Applying CALEA to the Internet In the Joint Comments filed November 8, 2004, CDT joined with a diverse group of industry and public interest organizations to argue that an extension of CALEA was not needed, was not supported by the factual record before the FCC, and was illegal under the terms of the CALEA statute itself.

The Joint Comments state that law enforcement access to Internet communications is important. Communications carried over the Internet are not - and should not be - immune from interception, nor should the Internet offer a safe haven for illegal activity. However, CALEA is a flawed statute that would be very harmful if applied to the Internet.

The Joint Comments make clear that, when Congress passed CALEA in 1994, it was a narrowly crafted statute, enacted to address concrete and documented problems carrying out wiretaps of phone conversations as digital switches and other new features were being introduced within the traditional telephone network, or PSTN. At the same time, however, Congress made clear that it was not regulating information services and the Internet. The Joint Comments details numerous ways in which the FCC's NPRM violates or misconstrues provisions of the CALEA statute.

The Joint Comments also argue that there is no factual basis for the intrusive regulatory scheme proposed by the FCC in its NPRM. Of greatest significance, there is no evidence that law enforcement has in fact encountered obstacles in intercepting Internet communications, or that more generally there is any concrete problem that needs to be solved. Under existing law, the FBI already can "wiretap the Internet," and service providers regularly work with law enforcement to satisfy lawful wiretap orders quickly and fully.

In contrast, an extension of CALEA would likely increase costs to consumers and businesses, impede innovation, and harm privacy and security. Imposing CALEA on the Internet in the manner proposed by the FCC would reverse more than a decade of sound policy decisions to allow the Internet to develop and grow without significant interference or constraint.

---

(4) Next Steps in FCC's Rulemaking Process On November 8, dozens of companies, public interest organizations, and individuals filed comments in the FCC's rulemaking proceeding. CDT will review the filed comments and will file "reply comments" responding to arguments raised by the Department of Justice or other commenters.

Reply comments can be filed with the FCC until midnight on December 7, 2004, and can be filed by anyone whether or not they filed an original comment. Reply comments, including brief individual comments, can be filed at http://www.fcc.gov/cgb/ecfs/ using "04-295" as the "Proceeding."

The Department of Justice's comments supporting the extension of CALEA, as well as a link to all comments filed with the FCC, are available at CDT's CALEA/VoIP Page: http://www.cdt.org/digi_tele/voip.shtml

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.20.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.20 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 21, December 6, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) US Weather Agency Embraces Open Internet Standards

On December 1, 2004, the National Oceanic and AtmosphericAdministration (NOAA) adopted a new policy of disseminatinggovernment-collected weather information using Internet standardsinstead of the proprietary standards that traditionally were accessibleonly by a small for-profit community.

NOAA's decision, designed to allow a broader range of private andpublic sector entities to easily use weather data, marks a watershed inthe dissemination of government-funded scientific and technicalinformation. It will strengthen the partnership among government,academia and the private sector, minimize the inefficiencies of theexisting system, and support the development of a wider range ofproducts and services using weather-related information. CDT hadsupported the change of policy, consistent with our goal of promotinguse of the Internet and opne standards to provide broader access togovernment information. CDT argued that improved data access wouldbenefit all participants in the weather enterprise by maximizing theaffordability, availability and usefulness of weather informationservices and by opening opportunities for new business models. CDT'scomments were cited in NOAA's final decision.

- NOAA's new Policy on Partnerships in the Provision of EnvironmentalInformation
  http://www.nws.noaa.gov/partnershippolicy/
- CDT's Comments to NOAA, June 30, 2004
  http://www.cdt.org/testimony/20040630cdt.shtml

---

(2) Background on Openness of Weather Information This summer, NOAA proposed a new policy that would "make its data and products available in Internet-accessible form ... based on recognizedstandards, formats, and metadata descriptions to ensure data fromdifferent observing platforms, databases, and models can be integratedand used by all interested parties in the weather, water, and climateenterprise." The existing weather reporting industry, including thecompanies that own the proprietary formats used today, argued againstdisclosure, asserting that it would put the government into unfaircompetition against the private sector.

On June 30, 2004, CDT filed comments at NOAA in support of the proposedpolicy, aarguing that it would strike a balance between (i) protectingthe rights of private companies that collect and disseminate data and(ii) ensuring unfettered access to information collected by thegovernment for the benefit of the public. CDT argued that taxpayersactually have been paying twice for weather data since taxpayers fundthe collection and then pay again to receive the results in theproprietary format.

Open Internet standards (such as those based on XML - "ExtensibleMarkup Language") offer an opportunity to make information widelyavailable and useful in a variety of applications. In this case, openstandards will support innovation, diversity and competition in thecreation of specialized weather products, tools, and models in theacademic and private sectors.

- "Who Owns the Weather?" - column by CDT Associate Director AriSchwartz for the Center for American Progress, July 28, 2004
  http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=131748

---

(3) NOAA's Move Follows a Positive Pattern in Release of GovernmentInformation The weather information debate was the latest in a series of strugglesover use of the Internet to disseminate government data that istechnically public but often locked up in proprietary formats. In 1993,public interest organizations won a long battle to convince theSecurities and Exchange Commission (SEC) to make its Electronic DataGathering and Retrieval System (EDGAR) freely available. The subsequentrelease of EDGAR on the Internet led to the creation of thousands ofnew services and sparked dramatic growth in the number of smallinvestors, who for the first time were able to easily look up marketnews and view SEC filings.

In 1998, a similar battle resulted in the release of the U.S. Patentand Trademark Office's database. The commercial providers of thisinformation had argued against making it freely available online, whilemost other business groups and public interest organizations pushed forits wide-scale release. Again, openness won out and the result wasmore private sector activity, not less. The new system has had littlenegative impact on businesses that conduct patent and trademarkresearch; it turns out that the basic information is not as importantto their profitability as the quality of their analysis. At the sametime, openness has brought greater accountability, as reporters andothers have used the information for investigations of patent claims.

CDT will continue to advocate for use of the Internet and open formatsto disseminate public information so it can be used in innovative ways.

- Securities and Exchange Commission: Important Information about EDGAR
  http://www.sec.gov/edgar/aboutedgar.htm
- U.S. Patent and Trademark Office Databases http://www.uspto.gov/patft/index.html

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.21.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.21 Copyright 2004 Center for Democracy and Technology

CDT POLICY POST
Volume 10, Number 22, December 6, 2004

A Briefing On Public Policy Issues Affecting Civil Liberties Online
from The Center For Democracy and Technology

---

(1) Intelligence Reform Bill Passes Congress, Ends Up A Mixed Bag for Civil Liberties

The House and Senate have voted to pass the much-debated intelligence reform bill, which responds at least in part to the recommendations of the 9/11 Commission. Several months ago, the House and Senate passed significantly different versions of the bill, and as late as last week it was unclear whether a final bill would be brought to a vote.

The 615-page legislation, which the President is expected to sign shortly, is a mixed bag for civil liberties. Many of the most egregious provisions contained in earlier provisions of the bill were removed, but other provisions that protected civil liberties also were removed or watered down.

Conference Report on and Text of Intelligence Reform Bill,
http://www.fas.org/irp/congress/2004_rpt/h108-796.html

---

(2) Civil Liberties Board Has Potential The intelligence reform bill creates a Privacy and Civil Liberties Oversight Board in the Executive Office of the President whose purpose is to ensure that privacy and civil liberties are considered in the policymaking process. Congress was responding to one of the recommendations of the 9/11 Commission Report, which acknowledged that counterterrorism efforts are leading to more powerful government powers and that "adequate supervision of the executive's use of powers to ensure protection of civil liberties" is necessary. Although some powers of the Board were weakened compared to an earlier Senate version, the Board has the potential to be an important force in protecting civil liberties if the White House gives the Board a role in the policymaking process, as Congress intended.

---

(3) Information Sharing Provisions Create Oversight, Privacy Protections The bill attempts to address one of the major problems in U.S. counterterrorism efforts: the failure of government agencies to share information and "connect the dots." It takes a comprehensive approach, requiring the Executive Branch to first develop a system design and privacy guidelines for information sharing. Modeled largely on the Senate bill, the provision calls for:

- a set of pointers and directories to information, which can be shared only with appropriate authorization;
- adoption of policy and privacy guidance before any system is built;
- a requirement on the front end of a system design plan weighing costs and impacts;
- phased implementation to allow congressional and public reaction; and
- the involvement of the civil liberties board to oversee and ensure privacy safeguards.

CDT urges Congress to continue to take a strong oversight role with regard to information sharing to ensure that appropriate safeguards are in place to protect civil liberties.

---

(4) Troublesome New Surveillance Authority in Legislation Although many "Patriot Act II" provisions did not make it to the final bill, a few of those sections survived. The "lone wolf" provision extends secret domestic intelligence surveillance under the Foreign Intelligence Surveillance Act to individuals without any suspected connection to a foreign terrorist organization or foreign government -- an unnecessary and potentially unconstitutional extension of government power. However, the legislation "sunsets" the lone wolf provision at the end of 2005, when some other surveillance powers in the USA PATRIOT Act expire.

---

(5) More Privacy Officers May Be On the Way One provision of the intelligence reform bill indicates the sense of Congress that agencies with law enforcement or counterterrorism responsibilities should designate privacy officers. A more substantive provision requiring privacy officers in departments and agencies was included in this year's omnibus appropriations bill, which the President signed into law today. Although it is unclear precisely what departments and agencies are covered, the two provisions taken together suggest that at least such entities as the Department of Justice, Department of Treasury and Department of State should have privacy officers.

---

(6) Other Provisions Have Civil Liberties Implications Other provisions of the bill also have civil liberties implications, both good and bad. The bill:

- requires that the Transportation Security Agency create redress procedures for airline passenger screening;
- clarifies and strengthens the roles of the Department of Homeland Security Privacy Officer, Civil Rights and Civil Liberties Officer and Inspector General in protecting privacy and civil liberties;
- requires additional reports to Congress about intelligence surveillance within the United States under the Foreign Intelligence Surveillance Act;
- expands sharing of grand jury information with foreign governments;
- requires the Attorney General to report to Congress about the process for doing criminal history background checks of job applicants for private employers;
- requires that cruise ship passengers be checked against terrorist watch lists; and
- increases funding for research into biometric-based mass identification technologies.

In addition, in order to pass the bill, Congress agreed to some basic national standards for driver's licenses and birth certificates, and agreed to debate other driver's license and identification-related issues next year.

Detailed information about online civil liberties issues may be found at http://www.cdt.org/.

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_10.22.shtml.

Excerpts may be re-posted with prior permission of ari@cdt.org

Policy Post 10.22 Copyright 2004 Center for Democracy and Technology