CDT POLICY POST
Volume 7, Number 1, February 8, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) CONGRESS EXAMINES ICANN DECISION-MAKING ON TOP LEVEL DOMAINS

Last year's selection of seven new global Top-Level Domains (gTLDs) by the Internet Corporation for Assigned Names and Numbers (ICANN) continues to generate controversy. On February 8, 2001, the Subcommittee on Telecommunications of the House Committee on Energy and Commerce held a hearing to examine the procedures of ICANN, the organization that oversees Internet domain names and other addressing functions.

CDT Associate Director Alan Davidson testified at the hearing, describing the public's interest in ICANN, and the ways in which that interest can be best protected.

The decision to adopt new gTLDs -- names that would join ".com," ".net," and ".org" as organizers of Internet content -- affects Internet users worldwide. The current gTLDs are highly congested and poorly differentiated, making it more difficult for users to find names that appropriately identify new online resources. New gTLDs, if properly introduced, could alleviate that problem and provide new opportunities for online expression. But a poorly managed rollout of new gTLDs could badly interfere with users' abilities to find and publish online content.

The gTLD decision, like many of ICANN's decisions, is therefore of public interest. CDT believes that ICANN has a responsibility to ensure that the public is well-represented when such decisions are made.

CDT's testimony is available at: http://www.cdt.org/testimony/010208davidson.shtml

---

(2) ICANN PROCESS UNDERREPRESENTS USER INTERESTS IN MAJOR ISSUES

Members of the Internet user community and advocates for user interests have been under-represented

throughout ICANN, and as a result have been excluded from important decisions. ICANN holds quarterly in-person meetings at locations all over the world, at which most of its major decisions are made. The expenses associated with physical attendance at such meetings place participation out of reach of many NGOs and public interest advocates. As a result, decisions made by the ICANN Board of Directors are made without benefit of broad input from the user community.

In theory, the ICANN Board of Directors includes representatives from the user community, but only five of the allotted nine seats for such "At-Large" Directors have so far been filled through online elections. Moreover, even the five elected Directors were not permitted to participate in ICANN's gTLD selection, nor have they participated in any of ICANN's decisions to date.

Besides the Board, ICANN also includes structures meant to encourage broad participation, but they do so only imperfectly. While ICANN explicitly provides representation to a number of commercial interests, it fails to represent properly the millions of individuals that own Internet domain names or have an interest in ICANN's decisions. The main outlet for individual participation -- the General Assembly of the Domain Names Supporting Organization -- appears increasingly ineffective. Non-commercial organizations have a constituency, the Non-Commercial Constituency, but it is only one of seven groups making up one of the three supporting organizations.

Overall, considering the broad impact of its decisions, ICANN does not presently provide adequate means for public input into its activities. CDT believes that major changes are necessary if ICANN is to achieve the degree of responsibility and legitimacy required for it to administer such important Internet functions.

---

(3) CDT ADVOCATES INTERNAL REFORMS TO ICANN STRUCTURE

For the last fifteen months, CDT has advocated strongly for broadly representative, fair mechanisms to provide this representation to ICANN. In March 2000, CDT and its partner Common Cause prepared a study of ICANN's election system, concluding that an "indirect election" system proposed by ICANN would not adequately represent the public's voice. In response, ICANN agreed to hold more democratic direct elections -- eventually held in October 2000 -- but has yet to settle on a permanent system to select "At-Large" Directors representing users.

CDT also believe that the process used to select gTLDs was flawed in this instance, and that reform is needed to ensure that all of ICANN's future decisions are transparent, objective, and obviously fair. Policies such as the non-refundable $50,000 fee ICANN requires just to apply for a gTLD need to be modified in such a way that ICANN is able to recoup its expenses without shutting the door on non-commercial applications. And, prior to making any decisions, ICANN should publish and adhere to a set of clear, objective criteria. Finally, ICANN should always provide full justification for its choices, so as to allow maximum opportunity for review and/or appeal.

Above all, ICANN needs to find ways to enforce a more limited mission statement. ICANN was designed as a technical management organization, not a policy-making institution for the Internet. Although some of its decisions may have policy implications, we believe ICANN is not equipped to make its choices based on anything but narrow, technical considerations. To its credit, the current ICANN Board has reiterated its desire to keep ICANN to a strictly technical mission and out of troubling policy matters. However, CDT believes that for ICANN to truly become both responsible and legitimate, it must adopt a three-pronged approach to its decision-making structure. First, and to the extent possible, ICANN must limit its activities to the purely technical. Second, ICANN needs to return to the bottom-up

consensus-building processes envisioned in its founding documents. Finally, ICANN should implement meaningful representation for the entire Internet community throughout its organization, so that the all of the diverse interests found on the Internet may contribute to ICANN's activities.

---

(4) INTERNATIONAL STUDY TEAM BEGINS EXAMINING AT-LARGE REPRESENTATION

CDT and a team of international researchers from the non-profit and academic community have recently begun examining the specifics of last year's ICANN election in order to identify areas of success and shortcoming. The study project, known as the NGO and Academic ICANN Study (NAIS), will examine the nature of public representation in ICANN, and will provide recommendations to the Board and the community. CDT and its partner Common Cause serve as project coordinators for NAIS, as well as North American researchers.

On February 7, the NAIS team transmitted a letter to the head of ICANN's own Study Committee, former Swedish Prime Minister Carl Bildt. In that letter, NAIS members requested that the Committee make important data from last year's election -- web logs, voting data, technical specifications, etc. -- available to the public for thorough evaluation. NAIS urged ICANN to be forthcoming with a wide variety of details from several months of voter registration and campaigning, while at the same time protecting the individual privacy of voters as fully as possible.

ICANN's first meeting of 2001 will be held in Melbourne, Australia, in early March. The NAIS team expects to hold a workshop immediately prior to the meeting, to inform the community about NAIS's progress and to solicit opinions about the direction of NAIS's work. The final NAIS report will be presented to the ICANN Board of Directors at ICANN's second meeting in Stockholm, Sweden, on June 4.

A copy of NAIS's letter to Carl Bildt is available at: http://www.cdt.org/dns/icann/nais/010207bildt.shtml

An overview of the NAIS project, including a list of participants, is available at: http://www.cdt.org/dns/icann/nais/010207overview.shtml

---

CDT POLICY POST
Volume 7, Number 2, February 16, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) SENATORS INTRODUCE RESOLUTION TO PUT MORE CONGRESSIONAL INFO ONLINE

Led by John McCain (R-AZ) and Patrick Leahy (D-VT), a bi-partisan group of Senators has introduced a resolution to put Congressional Research Service reports and lobbying disclosure records online. The bill, S. Res. 21, offers the best chance yet to make Congress more open and accountable.

The Congressional Research Service (CRS), housed in the Library of Congress, uses taxpayer dollars to produce reports on public policy issues ranging from foreign affairs to agriculture to health care. CRS reports represent some of the best research conducted by the federal government. All of the reports are posted online, but access is available only to Congressional offices through an intranet system. Citizens can order paper copies of the reports through their Member of Congress, but only by mail. Moreover, the general public cannot search through past reports, and a comprehensive index of the reports is not available online, so citizens basically have to guess when they ask for something.

CRS reports would be useful to researchers, students, librarians, government employees, and ordinary citizens. The McCain-Leahy resolution would put about 2700-2800 of these reports on the Internet. Despite co-sponsorship from Senate majority leader Trent Lott (R-MS), the measure faces an uphill battle, as a few key Senators continue to oppose it.

A letter endorsing the resolution, signed by over thirty public interest groups, including CDT, is at
http://www.congressproject.org/infopolicy/mccaincrsendor01.html

---

(2) CONGRESSIONAL RESEARCH SERVICE REPORTS STILL THE MOST WANTED

Forcing citizens to obtain CRS reports by mail rather than online is one example of Congress' continuing failure to take full advantage of the democratic potential of the Internet.

In August 1999, after consulting watchdog groups, reporters, librarians, and government employees, CDT and OMB Watch issued a report identifying the "Ten Most Wanted Government Documents" -- useful taxpayer-financed information that wasn't available online. http://www.cdt.org/righttoknow/10mostwanted/

Since our report's release, three of the most wanted documents have been placed online:

- Supreme Court Web site -- In a significant victory for government openness, the Supreme Court put up a Web site last summer. Public interest has been tremendous: the site received over one million visitors in the first few hours after the decision was posted in the Florida election case. http://www.supremecourtus.gov

- Endangered Species Recovery Plans -- These documents, which used to be available only for purchase, are now available in .pdf format directly from the Fish and Wildlife Service. http://endangered.fws.gov/recovery/recplans/index.htm

- Official Gazette of Trademarks -- Printed in compiled form, these documents were online in such a dispersed format that even officials at the US Patent and Trademark Office could not find them. They have since been linked to from a single location. http://www.uspto.gov/web/menu/og.html#tm

Unfortunately, Congress is lagging behind in putting up its information. In the CDT/OMB Watch survey, CRS reports were the #1 most wanted document government-wide. Two other important sets of Congressional information -- the full text of all Congressional hearings and a searchable database of Congressional votes -- also are still not online.

Reporter David Corn wrote an insightful article called "Filegate.gov" detailing Congress' unwillingness to use the Internet, in the November 2000 issue of Wired. Corn's article is available online at: http://www.wired.com/wired/archive/8.11/govdocs.html

---

(3) FRAMING AN E-GOVERNMENT AGENDA FOR THE 107TH CONGRESS

The early 1990s offered great promise for the federal government's use of the Internet. As early as 1995, most federal agencies had Web sites with information that had been previously available only in reading rooms in Washington or by mail under the Freedom of Information Act (FOIA). The Library of Congress' legislative information site "Thomas" http://thomas.loc.gov was seen as a revolutionary breakthrough for citizen interaction with government. In 1996, CDT was instrumental in securing passage of the Electronic-FOIA amendments, which required agencies to deliver documents in electronic format and to pro-actively post the most frequently requested documents.

However, after the passage of E-FOIA, the momentum to use the Internet to increase government openness slowed. This year, with the convening of the 107th Congress, CDT is seeing a renewed vigor among those interested in using the Internet to make government more responsive.

A full e-government agenda has yet to take shape. However, it should include the following initiatives, in addition to putting CRS documents online as called for in the McCain/Leahy resolution:

1. Allow citizens to opt for online responses to their FOIA requests - Citizens making FOIA requests should be able to specify that they want the government to respond by placing the information on the agency's Web site. This would not only make more information publicly accessible, but would likely save money by sparing the government the expense of having to copy and mail the same material over and over in answer to multiple requests.

2. Rewrite the Privacy Act and require "privacy impact assessments" for new information systems - Privacy has been shown to be the #1 reason that people are not using interactive services, yet the federal government is still operating under a Privacy Act signed into law in 1974. With the growth of the Internet, the Privacy Act needs a new look.

3. End the 60 day rule - Under Senate rules, Senators cannot make any changes to their Web pages within 60 days of an election, meaning that this most flexible and vibrant medium is frozen at the end of every term of Congress. Just when the most action is happening in Congress, Senators cannot use the Web to interact with constituents.

All of these reforms could -- and should -- be accomplished in this year. Other initiatives, such as taking advantage of new technologies such as XML to make government information more readily available to the public, will require more time but should be launched now.

For more information on updating the Privacy Act, see the Federal Computer Week article by CDT senior policy analyst Ari Schwartz at http://www.fcw.com/fcw/articles/2000/1030/pol-schwart-10-30-00.asp

For more information on the "60 day rule," see http://www.fcw.com/fcw/articles/2000/1211/pol-schwart-12-11-00.asp

---

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

CDT POLICY POST
Volume 7, Number 3, March 14, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) SEARCH CONTINUES FOR MEANINGFUL PUBLIC ROLE IN DOMAIN NAME MANAGEMENT

How can Internet users -- including individuals and small organizations -- have a say in the management of the Internet? Will the Internet's coming of age as a commercial medium give rise to gatekeepers unresponsive to the public interest?

The critical challenge of representing the public's voice in Internet management is posed most immediately today by ICANN, the Internet Corporation for Assigned Names and Numbers, the organization that manages domain names and addressing. Even such technical decisions can have far-reaching policy implications for free speech and privacy on the Internet.

This broad issue of the public interest in Internet management has led to CDT's ongoing participation in ICANN, which concluded its quarterly meeting early this week in Melbourne, Australia. Major topics of discussion at this latest meeting included the debate over public participation in ICANN's board, new proposals for management of the .com/.org/.net domains, and a range of other issues.

As part of an ongoing effort to study user participation in Internet management, CDT and a group of international researchers hosted a workshop in Melbourne on "The Future of the At-Large Membership & Public Participation in ICANN."

The workshop was convened by the NGO and Academic ICANN Study (NAIS), an ad hoc collaboration of nine research and advocacy groups from around the world, including CDT. The workshop discussed a critical debate at ICANN: The "At-Large" membership and elections for ICANN Directors that many view as an essential form of public participation in ICANN. NAIS is undertaking a far-reaching study of public participation in ICANN, and will be making recommendations regarding the future of ICANN's "At-Large" elections.

More information about the NAIS project is available at: http://www.naisproject.org/

Parallel to the NAIS effort, ICANN has appointed its own Study Committee to review the participation of the Internet community "At Large" in ICANN's decisions. On March 13, the ICANN Board of Directors

appointed six new members to its official effort.

While there has been criticism that the nine-member Study Committee includes too few advocates for public representation, members of the Committee have made clear that they intend to rely significantly on input from the Internet community in developing their recommendations. Several groups, including the NAIS team, have already announced their intention to provide such input to the Committee.

The terms of the Study Committee's work include a controversial "clean sheet" examination of public participation in ICANN -- thus re-opening the concept of including users in ICANN's decision-making. While such a broad scope gives the Study Committee flexibility to explore the rationale for public participation, it also requires advocates for public participation in ICANN to defend and define that interest vigorously.

In response to a letter from the NAIS group earlier this year, the At Large Study Committee has released a limited set of aggregate data about last October's At-Large election. While the data currently available is inadequate for a rigorous study of the election, CDT views it as a step in the right direction and hopes that the Study Committee will make further progress in the near future.

Information about the At-Large Study Committee, including biographies of its members and copies of the election data already made public, is available at: http://www.atlargestudy.org/

---

(2) BOARD TO CONSIDER NEW REGISTRY CONTRACTS, POSSIBLE ".ORG" RESTRICTIONS

Opening what could be a contentious debate, the ICANN Board discussed, but did not take final action, on a proposal to change ICANN's contracts with VeriSign, the company that manages the master list 'registry' of domain name registrations for the ".com," ".net," and ".org" top-level domains. Among other things, the proposal would require Verisign to divest the .net and .org registries sooner than otherwise expected but give the company a greater likelihood of retaining the .com registry in the future.

One feature of the new agreements would transfer control of the ".org" domain to a "sponsoring organization representing non-commercial organizations." ".org," like ".net" and ".com," is currently open to any individual, corporation or organization. Under the new proposal, ".org" could become a closed registry "operated by and for non-profit organizations." This raises difficult questions: What global definition of "non-profit" would be imposed on new .org registrants? What organization would decide and enforce such a policy? CDT fears that this proposal could ultimately do more harm than good to free expression on the Internet.

One of the Internet's most important features is the absence of gatekeepers with power to unjustly restrict online speech. Cheap, unfettered access to domain names empowers Internet users to establish online identities free from authoritarian interference. A decision by ICANN, however, to require domain name registrants to prove their standing as non-profit organizations could deny future registrants access to one of the Internet's longest-standing expressive spaces.

As a rule, CDT believes that unrestricted domain name spaces should play an important role in the future structure of the DNS. Since restricted spaces grant certain organizations authority to make binding decisions about who may or may not speak in a given online space, they are generally inconsistent with the basic values of openness that have promoted innovation and expression online. CDT hopes that ICANN will keep this tension in mind as it moves forward with negotiations for both present and future top-level domains.

The new contracts sparked intense debate in Melbourne, with comments noting both benefits -- such as the early recompetition of the .org and .net spaces -- as well as potential concerns about competition and the process and speed of the decision. While the Board postponed making a final decision, existing agreements require a decision by mid-April. In all likelihood, the ultimate decision will be made on a non-public ICANN Board teleconference in early April.

A description of the proposed changes is available at:
http://www.icann.org/melbourne/proposed-verisign-agreements-topic.htm

---

(3) DISCUSSIONS ON PRIVACY, NEW TOP LEVEL DOMAINS

Another pressing issue facing ICANN is the status of the publicly-accessible databases (so-called "WHOIS" data) of domain name owners' personal or corporate information. ICANN's contracts with the companies that register domain names for Internet users obligate the companies to provide free public access to the technical, administrative, and billing contacts associated with any domain name in ".com," ".net," and ".org." Such data is frequently used for technical maintenance of the network, law enforcement, and other purposes, but the freedom of its availability raises privacy questions when individuals find their home addresses, e-mail addresses and phone numbers used inappropriately. ICANN has established a WHOIS Committee but the absence of a well-defined user advocate makes it likely that broader policy issues regarding WHOIS will need to be worked out in another forum. CDT remains confident that processes can be put in place that provide needed access while preserving individual privacy.

Information on the .com/.net/.org WHOIS Committee is available at: http://www.icann.org/committees/whois/

The ICANN Board also discussed the state of negotiations between ICANN and the companies chosen in November 2000 to operate new global top-level domains (gTLDs) on the Internet. Four of seven negotiations for the new gTLDs are nearing completion and could begin accepting registrations relatively soon. Of these four new names -- .pro, .name, .info, and .biz -- only ".info" will be completely unrestricted. Draft versions of the necessary contracts were presented to the Board, although significant appendices remain to be released. The Board voted to authorize the ICANN staff to finalize negotiations and present contracts that would be adopted absent any further objection from Directors.

Agendas from the Board meeting and public comment forum, with links to the notes of the real-time scribe and copies of relevant documents, are available at:
http://cyber.law.harvard.edu/icann/melbourne/archive/index.html

CDT's ICANN page is http://www.cdt.org/dns/

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

CDT POLICY POST Volume 7, Number 4, June 1, 2001 A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY CONTENTS:

(1) LABELING MANDATES IN ANTI-SPAM LEGISLATION THREATEN FREE SPEECH.

Legislation currently under consideration in Congress to curtail spam - or unsolicited commercial electronic mail (UCE) - contains provisions that threaten free speech by, among other things, requiring labeling of UCE containing lawful "adult" material.

H.R. 718, introduced by Rep. Heather Wilson (R-N.M.), has gone through several versions. On Thursday, May 24, 2001, the House Judiciary Committee approved the bill. Key provisions of the bill make it a federal crime to intentionally transmit 10 or more unsolicited commercial email messages in a protected computer in the US knowing that the messages' header information "is materially false or misleading as to the identity of the person initiating the transmission."

While CDT has supported similar anti-spoofing provisions in the Senate, penalties provided for in the House bill are troubling. A first offense under this section is punishable by a fine and subsequent offenses may be punished by imprisonment for up to one year. In addition, ISPs could seek damages, with the total liability for any one misleading spam incident capped at $1 million.

More worrisome is an amendment adopted by the Judiciary Committee at the behest of Rep. Melissa Hart (R-PA) requiring that UCE containing adult content carry a header labeling it as such. Such a provision creates the threat of forced speech and stigmatizes potentially beneficial and lawful, though adult, speech. It also gives the Justice Department broad discretion to determine what is acceptable bulk mail and what is not.

The bill was previously reported by the House Commerce Committee with additional and controversial provisions making it illegal to send spam in violation of the terms of service of the recipient's ISP. See (4) below.

CDT believes that both the mandatory labeling provision and penalties in the Judiciary bill and the ISP terms of service provision in the Commerce Committee bill are unnecessary, out of proportion to the UCE problem.

H.R. 718 as introduced and reported by the Commerce Committee is available through CDT's Legislation page: http://www.cdt.org/legislation/107th/junkemail/.

(2) SPAM: A PROBLEM REQUIRING BALANCED SOLUTIONS THAT RESPECT FREE SPEECH

The efficiency of email - perhaps the Internet's most widely-used application - has brought with it some problems. Because a sender can almost effortlessly transmit a message to thousands, or even millions of recipients, the sending of UCE to vast email address lists has proven to be irresistible to some businesses.

However, unlike postal mail, the full cost of spam is not borne by the sender. Instead, the cost is shifted to intermediaries, such as Internet service providers (ISPs), and to recipients. While each individual email message only utilizes a minimal amount of Internet resources, when multiplied by the millions, such bulk messages can easily clog data pipelines and force both ISPs and recipients to spend time and resources to deal with what are frequently unwanted messages. Compounding the issue and raising the political heat is the use of UCE by purveyors of adult material.

In 1998, CDT coordinated an ad hoc working group on UCE, which submitted a report to the FTC concluding that there were ways to respond to UCE that were consistent with the First Amendment. The report found that a response to UCE should combine -

- Better technical tools and public policies that allow individuals to indicate their desire to receive or not receive UCE and exercise greater control over incoming email messages.
- Technical measures and public policies that prevent and/or prohibit the use of fraudulent headers to send unsolicited commercial email messages.
- Self-regulatory efforts to create opt-out or opt-in programs.
- Increased enforcement efforts, under existing laws, against email fraud.

The anti-spoofing provisions of HR 718, and similar provisions in the Senate legislation, are consistent with these principles. Mandatory labeling and federalization of ISP terms of service tip the balance too far and threaten First Amendment values.

The working group report on UCE is at http://www.cdt.org/spam/.

---

(3) MANDATORY CONTENT LABELING VIOLATES FIRST AMENDMENT

The House Judiciary bill as amended would mandate labeling of UCE that contains adult-oriented material.

This amendment, while targeted at pornography, would set a terrible precedent. It is fundamentally distinct from the requirement prohibiting false header information, which applies to all commercial email, regardless of content and which is subject to objective determination. In contrast, mandatory content labeling is a form of forced speech, which is as offensive to the Constitution as forced silence. And deciding when something is properly labeled or not involves the government directly in the type of picking and choosing among otherwise legal content that is also incompatible with the First Amendment

The amendment proposed by Congresswoman Hart and passed by the Judiciary Committee would require that senders of UCE label all email containing adult-oriented material. The amendment employs a standard provided many years ago for the Post Office in Title 39 of the United States Code, Section 3010, and "Mailing of sexually oriented advertisements." The standard for "sexually oriented material set forth in the statute is "any advertisement that depicts, in actual or simulated form, or explicitly describes, in a predominantly sexual context, human genitalia, any act of natural or unnatural sexual intercourse, any act of sadism or masochism, or any other erotic subject directly related to the foregoing."

While it may be appropriate to apply such a requirement to the paper mail system, long operated as a government monopoly and still highly regulated in many respects, such a standard is not transferable to Internet email. The Internet is entitled to the highest form of First Amendment protection, according to the United States Supreme Court in the Reno v. ACLU decision of 1997. Moreover, the anti-spoofing provisions of the legislation will go a long way toward effectively eliminating the kind of UCE this provision attempts to address.

Finally, it is crucial to note that this debate concerns only legal material. Distribution of child pornography and obscenity are already per se illegal, online as well as off, in which case labeling is not the issue.

---

(4) ISP TERMS OF SERVICE SHOULD NOT HAVE THE FORCE OF LAW

H.R. 718 as reported by the Commerce Committee also included a provision, not in the Judiciary Committee bill, that would make it illegal to send UCE that "uses the equipment of a provider of Internet access service," if such provider has in effect an anti-spam policy and has requested the sender not to use the equipment of the provider for the transmission of any unsolicited commercial electronic mail message.

In other words, sending email in violation of the policy of the recipient's ISP would violate federal law. Granting ISP terms of service the force of law in this way could create negative consequences for free expression and impose burdens on due process.

- While ISPs should be free to create their own terms of service in the marketplace, giving the force of law to ISP terms of service effectively allows commercial entities to create federal law without the scrutiny of the legislative process. For example, ISPs could decide not to accept certain labels; this provision would make doing so a federal crime.
- Because there is no oversight, ISPs will have latitude to set terms of service may include broad restrictions on UCE that impede speech and expression, and those terms of service will have the force of law.
- Giving force of law to ISP terms of service also raises issues of due process. Users and businesses would be required to know and adhere to the terms of service of each ISP that are subject to change without notice. In practical terms, when users send an email, they have no idea whether it violates their ISPs terms of service - in some cases users are not even aware of the identity of their ISP.

For more information about free speech and spam see: http://www.cdt.org/speech/spam/.

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 7, Number 5, June 8, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) DOMAIN NAME GROUP MEETS IN STOCKHOLM; PUBLIC ROLE, STRUCTURE DEBATED

The Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit group that coordinates aspects of the domain name system and other key Internet technical functions, held its quarterly meeting in Stockholm this week. Major topics discussed at the meeting included the ongoing debate over the public's role in ICANN, issues regarding ICANN's structure and mission as overseer of an authoritative root, and the future of the well-known .org domain.

---

(2) RESEARCH TEAM'S INTERIM REPORT CALLS FOR STRONG PUBLIC ROLE IN ICANN

The NGO and Academic ICANN Study (NAIS), a coalition of researchers from around the world including CDT, has released its first report on the role of the public in ICANN. Though preliminary in nature, the report finds that ICANN should include a strong measure of public input in its activities.

ICANN is the non-profit organization responsible for the technical management of some of the Internet's most important resources. Most notably, ICANN manages the Domain Name System that converts computer addresses like 206.112.85.50 into easily-remembered strings like www.cdt.org. Because ICANN's decisions affect the whole Internet, CDT and other organizations have strongly pressed it to include the interests of Internet users in its decision-making processes.

In its Interim Report, NAIS examined global experiences with last year's online election of five "At-Large" representatives to the nineteen-member ICANN Board of Directors. The 130-page Interim Report includes local perspectives on the election process from each of ICANN's five geographic regions, and the findings were presented at a public workshop in Stockholm on June 2. Also published was a ten-page Executive Summary describing the Interim Report's major findings, available in English and translated into French, Spanish, Italian, and Chinese.

The NAIS team will publish its Final Report on the public role in ICANN at ICANN's September meeting in Montevideo, Uruguay. The study is designed to parallel ICANN's own At-Large Study Committee, which will report to the ICANN board this fall. NAIS is fully independent both of the ALSC and of ICANN.

Electronic copies of the Interim Report, the Executive Summary, and information about the NAIS project are available at: http://www.naisproject.org/

---

(3) ACADEMICS, NGOS URGE SWIFT ACTION BY ICANN BOARD

At ICANN's four-day public meeting in Stockholm, CDT and representatives from NAIS emphasized the importance of rapid action by the ICANN Board of Directors to secure a system of public representation. Finding a role for the public voice is one of ICANN's highest priorities, yet, with the corporation now in its third year of operation, ICANN has yet to formally establish the rights and responsibilities of the Internet public in ICANN's operation. In fact, four seats on the Board originally reserved for "At-Large" Directors continue to be occupied by unelected individuals chosen at the time of ICANN's incorporation.

The Board is currently scheduled to take action on these issues at its Annual Meeting in November 2001, but there have been indications that some Directors are considering delay. Moreover, the current five "At-Large" Directors' terms of office will expire in November 2002. It is feared that further delay could jeopardize ICANN's ability to implement a selection system for directors in a timely way. A major finding of the NAIS report was that many were frustrated by election problems and a lack of outreach in last year's election, which were in turn caused in part by the tight timetable for implementing that election.

ICANN can only survive as an open and transparent organization, accountable to the Internet users and other interests affected by its decisions. It should resist the temptation to further delay fulfilling its responsibilities to the Internet community as a whole. CDT looks forward to working with the ICANN Board, staff, and all members of the ICANN community to bring about responsible reform in a timely fashion.

---

(4) OTHER ICANN ACTIVITIES IN STOCKHOLM

In other issues at the ICANN meeting in Stockholm, a group of representatives from the country-code Top-Level Domains (ccTLDs--the groups that administer country-specific Internet domains ending in ".uk" or ".jp" rather than ".com" or ".org") informed the ICANN Board that they would no longer participate in ICANN's Domain Name Supporting Organization, one of ICANN's major policy-making bodies. The ccTLDs provide a significant portion of ICANN's operational budget; their dissatisfaction with one of the core elements of the ICANN structure points to a need for substantial reform in ICANN's basic structure.

The three Supporting Organizations (S.0.s) are intended to be ICANN's main policy-generating bodies. They attempt to foster rough consensus in support of ICANN policies by bringing a wide group of technical, commercial, and non-profit stakeholders together for discussion and debate. However, the S.O. model--particularly in the case of the Domain Name Supporting Organization--has left many feeling disfranchised from the ICANN Board's important decisions. The ccTLDs' frustration with the S.O. structure is emblematic of the need for far-reaching ICANN reform that will make the organization more inclusive of all of the Internet's diverse communities.

Also in Stockholm, ICANN took the first step towards finding a new administrator for the popular .org domain space. Under the terms of a recent contract renegotiation with .org's current administrator, VeriSign, ICANN has been tasked with identifying or creating an entity--possibly a non-profit organization--to operate the domain when VeriSign's contract expires on 31 December 2002. In Stockholm, ICANN requested that the Domain Name Supporting Organization craft a recommendation on the matter for submission to the Board by mid-October 2001. Among the items at stake is a million fund earmarked for use by a non-profit .org operator.

Finally, the ICANN Board also approved the corporation's budget for fiscal year 2001-2002. ICANN's total operating budget increased 19.2% to about million, but the budget was criticized by many for failing to include a line item for expenses associated with implementing a system of public representation in the early part of next year. At the meeting, ICANN President/CEO Stuart Lynn indicated that such expenses, if necessary, would come from ICANN's administrative budget and operating reserve.

For more information about ICANN, visit CDT's ICANN page at: http://www.cdt.org/dns/icann/

CDT POLICY POST
Volume 7, Number 6, July 11, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) US Court Agrees to Hear Yahoo!'s Challenge to French Claim of Jurisdiction Yahoo! has cleared a key legal hurdle as it seeks relief in US courts from a French court ruling that set a dangerous precedent for speech and commerce online. The case arises from a decision by a French court in November 2000, which ordered Yahoo! to block French users from accessing auctions -- hosted on Yahoo's US-based servers -- of Nazi paraphernalia and other items.

On June 7, 2001, in the case of Yahoo! Inc. v. LICRA, a federal court in California denied a motion to dismiss Yahoo!'s request to declare the French ruling unenforceable. The California decision opened the way for the US court to take up the merits of Yahoo's claim that the French court exceeded its jurisdiction. The US court's opinion indicated that those who seek to use the foreign courts to control US-based Web sites will face legal challenges to enforcement of those judgments.

The background is this: Last year, a French court ruled that Yahoo!, by allowing its Web site to be accessed from France, ran afoul of France's law criminalizing the exhibition or sale of racist materials. In spite of arguments that it would be technologically difficult to block only French users, the French court ordered Yahoo! to implement the necessary technology, or face heavy daily fines. The court specifically directed Yahoo! to re-engineer its content servers in the United States and elsewhere to enable them to recognize French Internet Protocol addresses and block their access to Nazi material. It also required Yahoo! to ask users with "ambiguous" IP addresses to declare their nationality when they arrive at Yahoo!'s home page or when they initiate a search using the word "Nazi."

After the French court's ruling, Yahoo! filed a lawsuit in the federal district court in its home district in California asking for a declaratory judgment that the foreign verdict was unenforceable in the US. Yahoo!

argued that US courts should refuse to enforce the French judgment because it contravened fundamental US policy, namely, the strong protection of free speech offered by the First Amendment. Yahoo! pointed out that freedom of expression is recognized not only in the United States as a fundamental constitutional right, but also under international law. Yahoo! also argued that the French judgment conflicted with a US law that immunizes ISPs from liability for content that originates with third parties.

The US court ruling and the French Yahoo! decision, translated into English, can be found at http://www.cdt.org/jurisdiction/

---

(2) CDT Files Amicus Brief Highlighting Threat to Free Expression in Trans-Border Rulings This may seem a little convoluted -- a US court case seeking to block a French court decision. But the issue goes to the heart of the Internet freedom: Holding Web publishers in one country liable for simply publishing material that may be considered inappropriate when viewed by citizens of another country would chill free expression and commerce on the Internet. Online speech and commerce cannot be open and vibrant if governments can extend jurisdiction over foreign-hosted content.

The French Yahoo! ruling jeopardizes the Internet's unique ability to support free expression and other democratic values. Most countries have laws controlling some kinds of speech, but these laws vary widely based on culture. From country to country, prohibitions may cover sexually-explicit materials, hate speech, blasphemy, libel, certain kinds of advertising, national security information, or criticism of government officials.

When countries attempt to control content on the Internet by applying their domestic laws to speech originating outside of their country, the threat to freedom of expression is real. Imagine if every Web site were subject to the laws of all 180 countries in the world. Ironically, it would be the voices from poorer countries that might be stifled the most, as small creators of content would find it impossible to comply with so many different laws.

Making these arguments, CDT filed a "friend of the court" brief in support of Yahoo!, joined by the American Association of Publishers, the Freedom to Read Foundation, the ACLU, Human Rights Watch, People for the American Way, the Society of Professional Journalists, and others. CDT is following the case closely.

Yahoo!'s briefs, CDT's amicus brief, and other materials on the case are available at http://www.cdt.org/jurisdiction/.

---

(3) Exercise of Jurisdiction by Foreign Courts Seen in Other Cases Since the Yahoo! case, several other foreign court decisions held Web sites in other countries liable for content, illustrating the threat to freedom of speech online.

- The German Federal Court of Justice ruled that the country's legislation banning communications glorifying the Nazis and denying the Holocaust applies to all aspects of the Internet, no matter what their country of origin, or how the information is presented. The case concerned Frederick Toben, an Australian-based Holocaust revisionist who denied that millions of Jews died during World War II. Toben, who was born in Germany and carries an Australian passport, was found guilty in November 1999 of promoting his opinions on Holocaust denial through printed leaflets and Web pages. Sentenced to 10 months in prison, Toben appealed, arguing that since his Internet material was "printed" outside of

Germany, it was not subject to German legislation.

The Federal Court disagreed, and in doing so effectively set the precedent that all material published on the Web is subject to German legislation. In their ruling last December, Federal Court judges said that the laws prohibiting racial hatred clearly apply to Internet material created outside of Germany and stored on servers outside the country, but which is accessible to German Internet users.

- Also last year, an Italian appellate court ruled that Italy had jurisdiction over a libel case brought by an Italian citizen based on statements and images injurious to his reputation and privacy that had been posted on a Web site hosted outside Italy. The court found that a "theory of ubiquity" allowed the case to go forward on the ground that, while the offending conduct took place outside of Italy, the effects were felt within the country. The case was sent back to the Italian lower court for further investigation on the facts.

The Italian libel decision, translated into English, is posted at
http://www.cdt.org/international/001227italiandecision.pdf

---

(4) Key Issues of Jurisdiction Arising in National and International Forums When can one country impose its law on a Web site based in another country? This is one of the most complex issues in Internet policy today - with implications for consumer protection, intellectual property, and freedom of expression. The issue of extraterritorial control over the Internet is coming up repeatedly in a variety of contexts:

- France is considering a draft Information Society Law that would allow French judges to order ISPs to block the flow of data that is deemed offensive under French law. Under this proposal, Internet service providers would be civilly liable when they have been informed of apparently illegal content and have not deleted it or denied access to it. This proposal would apply not only to host providers, but also to access providers, in effect, codifying and extending the decision in the Yahoo! case.
- Meanwhile, an international body known as the Hague Conference on Private International Law has been drafting a convention that would set international rules for determining in which foreign country a party could be sued and when countries must recognize the judgments of foreign courts. The "Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters" is essentially designed to make it easier to enforce court rulings across borders. The treaty covers many kinds of civil lawsuits, and may include speech-related torts such as libel and defamation. Consumer groups and free speech activists have warned that the Convention may have a detrimental impact on Internet users, particularly with regard to freedom of expression.

For more information on the Hague Convention, go to http://www.cptech.org/ecom/jurisdiction/hague.html

- Finally, the US government has not maintained a consistent policy in this regard. While United States courts have repeatedly affirmed the importance of the Internet as a medium of communication and free expression, and have generally rejected attempts to censor online content, some in Congress and the Justice Department have wanted to control content on Web sites overseas, for example, in cases involving online gambling.

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

CDT POLICY POST
Volume 7, Number 7, August 30, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) MANY BANKS FALL SHORT IN PROVIDING ONLINE PRIVACY CHOICES TO CUSTOMERS Online banks are not giving consumers convenient, online opportunities to limit disclosure of their personal financial information, forcing customers to use more cumbersome offline mechanisms to opt-out of data sharing, according to a recent CDT study.

The study, released August 29, found that, of 100 banks studied that offer their customers the ability to open accounts online and use other banking services online (such as bill payment, mortgage quotes, and much more), only 22% provide their customers equally convenient online means of preventing information sharing with other companies.

Of greatest concern, the study found that several mortgage companies offering online services were not giving their customers any notice of their privacy practices. This seems to be in direct violation of the new federal banking law, the Gramm-Leach-Bliley Act ("GLB"), which went into effect on July 1.

CDT's report also found the surprising result that some of the bigger banks have the fewest online privacy options, with almost half offering little or no ability for customers to opt-out of information sharing with third parties.

But the news wasn't all bad. Some banks give customers a wide range of online and offline options for limiting disclosure of data. Among the banks that led the way with best practices were the Internet Bank, which promised not to share customers' information without their affirmative consent (opt-in), and First Union, which provides customers a secure online Web site to remove their information from various kinds of sharing and offers a toll free number for assistance as well.

Based on the results of the study, CDT made the following recommendations:

- Financial institutions should follow the best practices identified in the study. Thirteen institutions adhered to an opt-in policy for unaffiliated third-party sharing. Seven banks offered customers the opportunity to opt-out through a range of means, including the opportunity to opt-out online. Others should be living up to these standards, as a minimum.
- Policy makers should carefully consider the exceptions in the GLB law. Many large institutions that do not share information with third parties reserve the right to share with affiliates and "marketing partners" and the law allows them to do so without offering any opt-out.
- The Federal Trade Commission should look into the practices of the online mortgage companies that do not give consumers notice of their privacy practices. The FTC has oversight responsibility under the GLB law for various institutions, including the independent mortgage companies. These companies fared worst in the study.
- Policy makers considering broader Internet privacy legislation should learn from the lessons of the GLB Act. Requiring an opt-out choice for the financial industry has not yet given consumers easy-to-use controls over disclosure and use of personal financial information.

The full report, entitled "Online Banking Privacy: A Slow, Confusing Start to Giving Customers Control Over Their Information," is online: http://www.cdt.org/privacy/financial/010829onlinebanking.pdf [PDF- 7 MB]

---

(2) BACKGROUND ON BANKING PRIVACY Privacy, especially Internet privacy, has become one of the most important issues in the lives of Americans. At the same time, consumers are eager to take advantage of the convenience of online services, including online banking. Over a quarter of Americans who have gone online have used the Internet to bank or invest. Failure to address privacy concerns will hamper growth of this online marketplace and undermine the consumer trust that is essential to sustained online usage.

A recent attempt to address privacy concerns is the Gramm-Leach-Bliley Act of 1999 ("GLB"), which deregulated financial institutions and implemented a series of privacy standards that went into effect July 1, 2001.

Title V of GLB requires banks and other financial institutions to disclose to their customers their information gathering and sharing practices. Further, personal financial information may not be shared with unaffiliated third parties unless the customer is given an opportunity, commonly referred to as opt-out, to prevent such sharing. The law's opt-out requirement does not apply to the internal use of information and the sharing of information with affiliates and "marketing partners," allowing banks to share information with those entities without giving customers any choice. When the GLB law was passed, many advocates criticized these privacy provisions as too weak.

In recent months, as a result of GLB, almost every American has received one or more privacy notices in the mail from a financial institution such as a credit card company, insurance agent, stock broker or bank. Privacy experts have criticized these printed notices as complex and confusing.

Due to the unique concerns that Americans have with online privacy, CDT decided to look at how institutions offering online financial services were complying with the privacy provisions of GLB .

In particular, we wanted to see if financial institutions offering online services were also offering online privacy choices to their customers. In marketing online services, financial institutions consistently refer to ease and convenience. It seems only logical that the banks should provide consumers with a similarly convenient set of

privacy choices online. Our study found that many banks were missing an opportunity to make online opt-outs easier for consumers.

For more general information on financial privacy, see:

- The Privacy Rights Clearinghouse Financial Information Page: http://www.privacyrights.org/financial.htm
- Consumers Union's Financial Privacy Page: http://consumersunion.org/i/Financial_Services/Financial_Privacy/index.html

---

(3) CDT FILES COMPLAINT WITH FTC AGAINST ONLINE MORTGAGE COMPANIES In the course of surveying online financial institutions, we found that a number of online mortgage companies did not offer adequate notice of their privacy practices when they collected personal information from consumers. One, Sterling Mortgage, responded by promising to post a privacy policy soon. Five others did not respond, so we filed a complaint with the Federal Trade Commission, which has jurisdiction over online mortgage company compliance with GLB.

Our complaint asks the FTC to investigate and, if appropriate, order the companies to post the required privacy policy or take other action as required by law.

The five companies named in the complaint are

- Advantage Mortgage
- Ameriwest Mortgage
- Central New England Mortgage
- G.M. Mortgage
- Online Mortgage Corporation

In recent years, the FTC has shown growing interest in privacy issues. The new Chairman of the Commission has expressed an interest in receiving specific complaints about privacy violations. CDT will be on the lookout for other privacy violations that merit the Commission's attention.

The CDT complaint is online at http://www.cdt.org/privacy/financial/010829ftc.shtml

---

(4) ONLINE PRIVACY ISSUES MAY HEAT UP WHEN CONGRESS RETURNS Consumer privacy issues, which were high on Congress' agenda at the end of last year, seemed to have fallen in priority this year, but that may change with Congress' return next week from its August recess.

In the Senate, several privacy bills have been introduced, but the major actors from last year, including the Commerce Committee Chairman and Ranking Member Senator Fritz Hollings (D-SC) and Senator John McCain (R-AZ), have not yet introduced legislation. However, the Commerce Committee's recent hearings revealed intense interest on the part of a number of Senators. CDT expects to see further legislation introduced in the next couple of months, along with efforts to develop a set of protections that could attract wide sponsorship.

The House Commerce Committee has held several hearings on various online privacy issues. Senior Republicans are likely to introduce a bill this Fall, but efforts at a bi-partisan approach have yet to begin.

You can follow the major online consumer privacy bills at CDT's Privacy Legislation Page -- http://www.cdt.org/legislation/107th/privacy/

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

CDT POLICY POST
Volume 7, Number 8, September 24, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) PRESERVING DEMOCRATIC FREEDOMS IN TIMES OF PERIL The Center for Democracy and Technology joins the nation in grief and anger over the devastating loss of life resulting from the terrorist hijackings and attacks against the World Trade Center and the Pentagon. We too had friends killed on September 11. We fervently support the efforts of our government to hold accountable those who directed and supported these atrocities.

Responding to these terrorist attacks and the threat of future ones will test our Nation's collective resolve to maintain the freedom, openness and diversity that defines and enriches our society. At CDT, as we analyze policy proposals emerging in response to the September 11 attacks, we are guided by three convictions:

- surrendering freedom will not necessarily purchase added security;
- democratic values are strengths, not weaknesses; and
- open communications networks are a positive force in the fight against violence and intolerance.

It is clear that improvements need to be made in America's counter-terrorism procedures. But we know from history that measures undertaken in times of peril often infringe civil liberties without enhancing security. In the current climate, it is all the more important to act deliberately and ensure that our response is balanced and properly targeted. If we give up the constitutional freedoms fundamental to our democratic way of life, then the terrorists will have won.

---

(2) CONGRESS AND BUSH ADMINISTRATION RUSHING TO DEVELOP LEGISLATIVE PROPOSALS Lawmakers are scrambling to react to the September 11 terrorist attacks. Many of the proposals relate to the electronic surveillance laws and the system that gives different powers and sets different standards for the law enforcement agencies, such as the FBI, and the intelligence agencies, such as the CIA. While members of Congress from across the political spectrum have expressed concern about the effect that some of these proposals may have on our basic freedoms, the number and complexity of proposals and the speed with which they are being considered makes it very difficult to assess their impact.

Already, on September 13, the Senate adopted legislation giving government agencies somewhat broader authority to conduct certain kinds of electronic surveillance.

On Monday, September 24 at 2:00 pm, the House Judiciary Committee will be holding a hearing on the Bush Administration's anti-terrorism proposals. The only witness will be Attorney General Ashcroft.

Following this hearing, at 4:30 pm, the Committee expects to hold a closed hearing ("briefing") at which a panel of experts with civil liberties concerns will testify before the Committee. Witnesses will be : Jim Dempsey, CDT deputy director, focusing on the electronic surveillance issues; Prof. David Cole, Georgetown University Law Center, focusing on immigration issues; Brad Jansen, Free Congress Foundation on money laundering and forfeiture; Rachel King from the ACLU on criminal justice issues; and Morton Halperin of the Council on Foreign Relations on intelligence agency issues.

On Tuesday, September 25, the full Judiciary Committee will hold a markup on the Administration's bill with the hope of reporting out of the committee on that same day. Chairman Sensenbrenner expects the package to be on the Floor the following week.

Also on Monday, September 24 at 3:00 pm, the Senate Intelligence Committee is holding a hearing. CDT Executive Director Jerry Berman will testify.

It is also expected that the Senate Judiciary Committee will hold a hearing on Tuesday, September 25.

---

(3) CDT'S NEW "RESPONSE TO TERRORISM" RESOURCE PAGE To assist Netizens in following legislative developments, CDT is compiling the key documents on the issue in a "Response to Terrorism" resource page - http://www.cdt.org/security/010911response.shtml.

This page, which is being updated regularly, includes:

- The Administration's bill and other legislative materials.
- Analyses by CDT and other organizations.
- Statements and other background materials.

---

(4) WHAT YOU CAN DO! With time running short, we are recommending that concerned citizens do two things as soon as possible:

1. Endorse the "In Defense of Freedom" statement --

This statement -- already signed by more than 150 organizations (including CDT), 300 law professors, and 40 computer scientists -- calls on lawmakers to consider proposals calmly and deliberately with a determination not to erode the liberties and freedoms that are at the core of the American way of life. Individuals can read and endorse the statement by going to http://www.cdt.org/action/indefenseoffreedom/.

- Call your Members of Congress in Washington --

Tell your representatives that you want action to be taken, but it must preserve privacy and other basic freedoms.

CDT has a resource to help you find the contact information about your representatives in Washington -- http://www.cdt.org/action/contactcongress.shtml.

Members of CDT's Activist Network will be receiving an additional "Action Alert" with more information.

You are currently not a member of the Activist Network, but you can sign up easily at http://www.cdt.org/join/.

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

CDT POLICY POST
Volume 7, Number 9, September 26, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) CFP2002 SET FOR SAN FRANCISCO: PROPOSALS WANTED; OCTOBER 15 DEADLINE The Computers, Freedom and Privacy Conference (CFP) is a leading annual venue for public debate on issues relating to the future of privacy and freedom on the Internet. CFP 2002 is scheduled for April 16-19, 2002 in San Francisco. Given the grief and anger we feel about the September 11 terrorist attacks and the frenetic policy debates underway in Washington, it is hard to look forward as far as next April. But CFP has always been an important opportunity to consider the future of the Net, and to make it successful planning must proceed. CDT is actively involved in the conference's preparations. Associate Director Ari Schwartz is serving as Conference Chairman for CFP 2002. CDT also supports CFP through in-kind sponsorship.

The program committee is seeking proposals for innovative conference sessions and speakers. While proposals are welcomed on all aspects of computing, freedom, and privacy, the organizers encourage proposals that explore some of the most important issues facing the Internet and freedom, including:

- global activism;
- technology and monopoly;
- voting technology and democracy; technology and weapons;
- ICANN and Internet governance;
- borders and censorship;
- digital divide;
- biometric systems;
- consumer privacy;
- wireless privacy and security;
- hacktivism;
- intellectual property and intellectual freedom;
- digital rights management and privacy;
- public records and private lives.

Proposals are due by October 15, 2001. See http://www.cfp2002.org/participation/ for more information.

For more general conference related information, please visit the CFP web site at http://www.cfp2002.org.

---

1. A workshop entitled "Fair Use By Design?" will explore the impact of digital rights management tools specifically on "fair use." The discussion will focus on the limitations, contextual requirements, and barriers to fair use that are created by digital rights management technology. For more information please visit the CFP web site at http://www.cfp2002.org/participation/#workshop.

2. CFP encourages student attendance. Full time college or graduate students may apply for financial support to attend the conference. Application information will be available in mid to late fall 2001. Check the CFP web site at http://www.cfp2002.org for updates.

3. In an effort to enlarge the number and variety of groups and organizations engaged in technology related policy issues, CFP will offer a few scholarships to be awarded to those community groups who have been underrepresented at past CFP conferences. Application information will be available in mid to late fall 2001. Check the CFP web site at http://www.cfp2002.org for updates.

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

CDT POLICY POST
Volume 7, Number 10, October 9, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) SURVEILLANCE BILLS MOVE THROUGH HOUSE AND SENATE Legislation to expand government surveillance and access to stored data may be considered by the House and Senate in the next several days. The House Judiciary Committee marked up its bill last week, on October 3, while on Friday, October 5, Senate Judiciary Committee Chairman Patrick Leahy introduced a bipartisan bill that may go straight to the full Senate.

Following the attacks of September 11, it is clear that US anti-terrorism efforts need to be improved. The seriousness of the issue demands that whatever is done be effective and focused without unnecessarily infringing civil liberties . Unfortunately, there has been little time for deliberation. The Bush Administration came forward soon after the attacks with a long list of proposals, some of which involve quite fundamental changes in the surveillance laws, particularly as they relate to intelligence investigations in the US. Most of the Bush changes are not limited to terrorism cases, but concern all crimes and all intelligence investigations.

CDT has been tracking these issues and offering its recommendations for balancing national security and civil liberties. We have established a special page where we are posting the latest draft bills, analyses, testimony and other materials, updated on a daily basis: http://www.cdt.org/security/010911response.shtml

In this Policy Post, we summarize the main issues of concern to privacy, online and off, in the pending legislation.

---

(2) ANTI-TERRORISM LEGISLATION WOULD THREATEN PRIVACY ON THE INTERNET Two provisions in the House and Senate bills directly and specifically affect the Internet.

- Pen Registers/ Trap and Trace Devices for the Internet (House 101, Senate 216) - Allows government to collect, in real-time, unspecified, undefined information about Web browsing and e-mail without meaningful judicial review. This provision takes an already ambiguous statute and makes it more ambiguous, while giving the government a basis to claim access to more Internet transactional information.
    - Expands "rubber-stamp" authority of the pen register statute (designed to collect telephone dialing information) to "dialing, routing, addressing and signaling information" regarding e-mail, Web browsing and other Internet use.
    - Excludes "content," but no one knows what that means on the Internet, where packets combine content and non-content, and signaling data reveal much more than telephone numbers do. No definition is given to the terms "routing, addressing and signaling."
    - Will be cited by FBI in imposing Carnivore on ISPs and others.
    - At the least, it needs to be made clear that URL information after the host name (everything after cnn.com or amazon.com) is content that cannot be intercepted by pen register.
- Interception of computer trespasser communications (House 105, Senate 217) - Allows ISPs, universities, network administrators to authorize surveillance on others without judicial order.
    - Says that anyone accessing a computer "without authorization" has no privacy rights and can be tapped by the government without a court order, if the operator of the computer system says its okay. "Without authorization" is not defined.
    - Under the House version, relatively minor violations - like downloading a copyrighted mp3 file - would allow an ISP to authorize the government to tap all of that person's communications. With no judicial permission, oversight, or supervision.
    - No time limit - the extrajudicial wiretapping could go on for ever.
    - Senate bill states "computer trespasser" does not include any person with a "preexisting contractual agreement" with the computer operator, thus exempting ISP users. Senate language is better and should be expanded to deal with workplaces, universities, libraries, or other network operators who do not necessarily have a contractual relationship with their users. Provision also needs to be given a time limitation of 48 hours, the limit on other emergency wiretap authorities.

---

(3) FUNDAMENTAL CHANGES PROPOSED IN INTELLIGENCE AUTHORITIES Since the 1970s, our government privacy laws have been founded on a distinction between law enforcement and intelligence. The FBI, acting as an intelligence agency has broad powers, exercised largely in secret, to wiretap, conduct secret physical searches, and compel disclosure of financial, credit, travel and other records. Standards have been built up to govern use of those authorities, but they are looser than the standards governing access in criminal cases. Part of the justification for these lower standards was that they would be used in connection with foreign policy, national defense and diplomacy, not for the purpose of gathering evidence in criminal

cases.

Now, the Administration is asking Congress to lower the standards for intelligence investigations even further and, at the same time, to allow these authorities to be used for the purpose of gathering evidence in criminal cases, thus circumventing the stricter procedures. The changes include:

- Eliminating FISA's "primary purpose" test (House 153, Senate 218) -- Criminal wiretaps could be conducted under the lower standards for foreign intelligence, without showing probable cause of a crime -- an end-run around the relatively more stringent requirements for wiretaps in Title III.

- Eliminates the requirement that FISA procedures only be used when the government's purpose is the gathering of foreign intelligence -- allows wiretaps and secret searches in criminal investigations under the weaker FISA standards thereby circumventing the relatively stricter requirements for criminal investigations.

- The latest language in the bills - which adds the word "significant" - is characterized as a compromise but would in fact have the same effect as the administration proposal. It would authorize the use of FISA procedures in all criminal investigations involving international terrorism or espionage, because they will always have "a significant' foreign intelligence gathering purpose. Destroys the distinction between intelligence and law enforcement agencies, which made the lower standards of FISA constitutional in the first place.

- Roving taps in FISA cases (House 152, Senate 206) - Allows FBI to go from phone to phone, computer to computer, without assurance that device is used by suspected terrorist. Gives FBI multi-point or "roving" tap authority in FISA cases. But does not limit tap top phone or computer while suspect is using it.

    - Could allow government to tap all the computers in a library if suspect is using one of them. If a FISA target is using payphones, the government could tap all payphones in the neighborhood, all day long.

    - House Judiciary Committee Members agreed to work to include the so-called ascertainment guideline, which is in the roving tap provision applicable in criminal cases, specifying that the government can tap a particular payphone or computer when it ascertains that the target is using it.

- FISA Business Records Provision (House 156, Senate 215) -- Overrides existing privacy laws for sensitive categories of records, including medical, educational and library. Would give intelligence agency access to "any tangible thing" - including sensitive medical, financial, or library records - from any person, with minimal judicial review, if "sought for" an intelligence investigation. A simple change - "Unless existing federal or state law provides otherwise as to the criteria for obtaining an order to produce records," - would avoid preemption of existing privacy laws.

- Sharing of Intelligence Information (House 103, 154, 353; Senate 203) - Allows intelligence agencies to receive - mainly with no judicial controls - information collected domestically in criminal cases.

---

(4) SECRET SEARCHES OF HOMES AND OFFICES SOUGHT In a provision that would codify a highly contested area of the law, the Senate bill would allow law enforcement agencies to search homes and offices without notifying the owner right away. (Senate 213, not in the House bill)

- Not limited to terrorism cases - emerged two years ago in an anti-methamphetamine bill. Applies to citizens. See August 20, 1999 Policy Post http://www.cdt.org/publications/pp_5.19.html Allows seizure of things and of wire and electronic communications (thereby seeming to supercede Title III.)

- Government could enter your house, apartment or office with a search warrant when you are away, search through your property and take photographs, and in some cases seize physical property and electronic communications, and not tell you until later.

The Senate made changes to the broad Administration proposal, but secret searches remain a fundamental departure for traditional police practice and strict adherence to the Fourth Amendment. This provision should be dropped.

---

(5) BUSH ADMINISTRATION REJECTS COMPROMISE A lot of Members of the House and public interest groups worked very hard to make improvements (some would say marginal improvements) in the anti-terrorism bill in the House. Chairman F. James Sensenbrenner worked in good faith with ranking Democrat John Conyers, Jr. to follow normal legislative procedure, including a mark-up.

Most notable among the compromises made, the House bill's surveillance provisions "sunset" in two years.

As CDT and other groups from across the political spectrum have pushed for a balanced bill that addresses civil liberties concerns, the Department of Justice has made it clear that it wants all the new authorities made permanent and that it is unwilling to accept meaningful judicial controls or otherwise compromise. In its latest move, the Administration is actually working to preclude the House from voting on the anti-terrorism bill as reported from the House Judiciary Committee.

Over the Columbus Day weekend, the Administration began pushing for a delay in consideration of the House bill, with the goal of getting the House to accept provisions of the Senate bill and otherwise return to the Administration's initial proposals. This approach - delaying until it gets everything its way - belies the Administration's claim that it needs these new authorities to respond to an emergency.

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

CDT POLICY POST
Volume 7, Number 11, October 26, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) ANTI-TERRORISM LEGISLATION GUTTING PRIVACY STANDARDS BECOMES LAW President Bush on October 26 signed into law an anti-terrorism package that dismantles many privacy protections for communications and personal data. Many of the provisions are not limited to terrorism investigations, but apply to all criminal or intelligence investigations.

This bill has been called a compromise but the only thing compromised is our civil liberties.

The bill:

- Allows government agents to collect undefined new information about Web browsing and e-mail without meaningful judicial review;
- Allow Internet Service Providers, universities, network administrators to authorize surveillance of "computer trespassers" without a judicial order;
- Overrides existing state and federal privacy laws, allowing FBI to compel disclosure of any kind of records, including sensitive medical, educational and library borrowing records, upon the mere claim that they are connected with an intelligence investigation;
- Allows law enforcement agencies to search homes and offices without notifying the owner for days or weeks after, not only in terrorism cases, but in all cases - the so-called "sneak and peek" authority;
- Allows FBI to share with the CIA information collected in the name of a grand jury, thereby giving the CIA the domestic subpoena powers it was never supposed to have;
- Allows FBI to conduct wiretaps and secret searches in criminal cases using the lower standards previously used only for the purpose of collecting foreign intelligence.

The text of the legislation and analyses by CDT and others are online at

(2) PROVISIONS TAKE EFFECT IMMEDIATELY; SOME "SUNSET" IN 2005 As passed, some of the surveillance provisions expire, or "sunset," in four years unless renewed by Congress. In four years, before any extension of the provisions, CDT hopes that there will be a Congressional review that will involve the deliberative balancing of civil liberties and national security that was lacking from the current debate.

CDT made it clear throughout the debate that terrorism was a serious problem, that the U.S. counter-terrorism effort had failed on September 11, and that changes to government security programs were needed. What is doubly distressing about the new law is that it was enacted without any examination of why existing authorities failed to prevent the September 11 attacks.

It is our greatest concern that the changes will be worse than ineffective - that, by cutting government agencies loose from standards and judicial controls, they will result in the government casting an even wider net, collecting more information on innocent people, information that distracts the government from the task of identifying those who are planning future attacks.

The sunset provision does not apply to the sharing of grand jury information with the CIA, giving the CIA permanent benefit of the grand jury powers. Nor does it apply to the provisions for sneak and peek searches or the provision extending application of the pen register and trap and trace law to the Internet.

The sunset also does not apply to ongoing investigations. Since intelligence investigations often run for years, even decades, the authorities will continue to be used even if they are not formally extended in 2005.

---

(3) NEW LAW REQUIRES CLOSE OVERSIGHT; OTHER CIVIL LIBERTIES ISSUES LOOM Many threats to civil liberties loom in the short and mid-term. CDT is planning a series of efforts to monitor implementation of the new law as well as to counter additional efforts to erode privacy and other civil liberties:

- CDT is calling upon Congress to exercise its oversight powers to conduct a probing and sustained review of how the new law is interpreted and applied. To that end, CDT will be working, through its Digital Privacy and Security Working Group, to share information among affected members of the telecommunications and Internet industry and other civil liberties groups. The co-chairs of the Congressional Internet Caucus have asked CDT to use DPSWG and the Internet Caucus Advisory Committee to examine the new law and future proposals.

- The FBI may be pushing for extension to the Internet of the Communications Assistance for Law Enforcement Act, the 1994 law requiring telecommunications carriers -- but not providers of information services -- to build surveillance capabilities into their networks. Implementing CALEA in the traditional and wireless telephone networks has proven extremely contentious. Extending it to the Internet could have even worse consequences for network operations and security.

- CALEA for the Internet is only one shape that design mandates may take. European governments have been particularly aggressive in pushing data retention requirements -- rules requiring ISPs and others to maintain logs of all communications for a period of months. The issue of critical infrastructure protection also could serve as a vehicle for government controls on technology.

- Calls have been made for a national ID card. In addition to the civil liberties implications of hard copy identity cards, the concept poses additional risks if extended to the Internet. Several bills have been introduced or are being drafted calling for greater use of biometrics at the borders and in other contexts.

- Encryption is not entirely off the agenda. While Senator Judd Gregg pulled back from his announced intent to introduce mandatory key recovery legislation, the issue may return.

- At the behest of the new cyber-security czar, NSC official Richard Clarke, the Bush Administration issued a Request for Information (RFI) to the U.S. telecommunications industry seeking information and suggestions for the development of a special telecommunications network, separate from the Internet. The proposal's impact on e-government and citizen access to information is unclear, and it raises questions about the lack of government confidence in, and commitment to, the Internet.

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

CDT POLICY POST
Volume 7, Number 12, November 1, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) DEPARTMENT OF COMMERCE SELECTS .us OPERATOR The U.S. Department of Commerce has selected NeuStar, Inc., as the new registry operator for the .us Internet domain. Like .com and .org, .us is a space on the Internet in which web pages and other resources are located. But unlike those globally-oriented domains, .us is intended to be exclusively for Internet resources that are American in nature.

The Department of Commerce's announcement is the culmination of a proceeding that began in June 2001. At that time, CDT joined a coalition of concerned non-profit groups, companies, community groups, and government agencies to advocate responsible, fair policy-making practices for .us. The coalition proposed to cooperate with the .us registry operator to create a .us "Policy Development Council" (usPDC) that would include a broad diversity of perspectives, to help resolve difficult policy questions.

While NeuStar has indicated a willingness to implement good policy practices in .us, it has not yet committed to any specific course of action, or to cooperation with any of the partners in the usPDC coalition. Over the next few weeks, CDT and its coalition partners hope to work with NeuStar and the Commerce Department to ensure that .us's policy processes are in keeping with democratic values.

On November 1, the House Energy and Commerce Committee Subcommittee on Telecommunications and the Internet held a hearing substantially focused on the .us proceeding and specifically on the possibility of creating a .kids or .kids.us domain for child-friendly material. CDT issued a letter raising questions about whether .kids could be properly and fairly implemented.

Additional information about the Commerce Department's award of .us is available at: http://www.ntia.doc.gov/ntiahome/domainname/usca/index.html.

CDT's letter to the Subcommittee on Telecommunications and the Internet regarding the proposed .kids legislation is available at: http://www.cdt.org/dns/011031dotkids.shtml.

More information is available at: http://www.cdt.org/dns/.

---

(2) NET MANAGING BODY LIKELY TO FOCUS ON SECURITY, DELAY PUBLIC INPUT DECISION The group that manages some of the Internet's most critical functions has indicated that it will delay a long-scheduled decision on how (and whether) Internet users will have a voice in policy discussions that affect the Internet worldwide.

The Internet Corporation for Assigned Names and Numbers (ICANN) manages the naming and addressing systems that make the Internet run smoothly and reliably. ICANN also makes important policy decisions like adding new domains to the Internet -- such as the recently-activated .info and .biz -- or maintaining trademark protections online. CDT strongly believes that the broad impact of ICANN's policy powers creates a need for Internet users to be strongly represented in ICANN's processes.

The question of public participation has been a defining one since ICANN's creation in 1998. ICANN's Board since then has been dominated by Internet companies and other private actors who do not have the mission of representing the public interest, and the public role in ICANN, while frequently alluded to, has not been defined in any of ICANN's organizational documents.

The Board was expected to resolve this question at its upcoming annual meeting in Marina del Rey, California, on November 12-15. In the wake of the September 11 attacks, however, it has indicated that it will not do so, and will instead change its agenda to focus on issues of security. ICANN has also asked that its stakeholder constituencies be prepared to make their own reports on how they are promoting security in the Internet's core systems.

Security of the Internet's naming and addressing systems is one of ICANN's most important and appropriate responsibilities, and CDT believes this is a fitting time for ICANN to take up the issue. However, the ICANN Board and the entire ICANN community must resist the urge to allow such immediate issues to derail other long-standing and important questions. ICANN must commit itself soon to resolving too-long-outstanding questions about the public's interest in Internet policy.

Information on the November meeting of the ICANN Board: http://www.icann.org/mdr2001/

---

(3) STUDY RECOMMENDATIONS RAISE QUESTIONS, LIMIT USER VOICE Last year, the ICANN Board commissioned a study to examine issues of public participation, stating that it would make its decision when that study was complete. That study group (known as the At-Large Study Committee (ALSC)) released a short initial report in early September; a final report is due in November.

The ALSC's September draft report would greatly restrict users' participation in ICANN. Most troublingly, the ALSC recommended that the number of publicly-elected seats on ICANN's nineteen-member Board be reduced from the current nine to six. This reduction would mean that all ICANN policy decisions, no matter how sweeping (even including changes to ICANN's basic mission and authorities), could be passed by corporate and technical representatives over the unanimous objection of the Board's publicly-elected Directors.

The report also recommended that voting rights in ICANN be limited to owners of Internet domain names and payment of some not-yet-described membership fee. In CDT's view, ICANN affects all users of the Internet, not just those who own domain names. By limiting the public voice in ICANN, the ALSC recommendations would put ICANN beyond the control of the people affected most by ICANN's activities. In CDT's opinion, such an approach would threaten the Internet's openness and empowering potential. Membership fees pose the danger of disenfranchising Internet users from the developing world.

These and other recommendations by the ALSC stand in contrast to the conclusions of the NGO and Academic ICANN Study, an independent, international study of ICANN (of which CDT was a member). The NAIS report, issued in June 2001, advocated a more open, responsive vision of ICANN in which voting rights are available to all Internet users with an interest in participating and who have verifiable e-mail and postal addresses. The NAIS report recommended an ICANN Board of Directors that balances private technical and professional interests with elected representatives of the public interest.

The ICANN ALSC draft report is online at http://atlargestudy.org/

The NAIS report is online at http://www.naisproject.org/report/final/

---

(4) ICANN REQUIRES LIMITS TO ITS AUTHORITY, REAL ACCOUNTABILITY Since hundreds of millions of users depend on ICANN-managed systems for smooth Internet access, ICANN's potential authority to affect the Internet as a whole is very broad. Right now, there are no effective controls to keep ICANN from abusing that authority some time in the future. CDT believes that, if ICANN is to safely serve the global Internet community, its activities must be constrained to the technical management for which it was designed.

These constraints should include:

- changes to the ICANN bylaws and to its charter that would affirmatively prevent ICANN from venturing into obvious policy-making;
- an independent review panel, empowered to monitor and even overturn ICANN decisions that are contrary to the best interests of the Internet;
- strong statements of Internet users' rights before ICANN, such as the right to be free of ICANN interference in matters of free expression or privacy.

These and other steps were recommended by CDT and Common Cause in a joint report issued in March 2000: http://www.cdt.org/dns/study.shtml

---

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

CDT POLICY POST
Volume 7, Number 13, November 12, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) PROPOSED "OPES" PROTOCOL ADVANCES; POLICY ISSUES TO BE CONSIDERED As part of a major new project to increase the public voice in Internet standards setting processes, CDT has been engaged in the debate about a proposed new Internet protocol named "Open Pluggable Edge Services" ("OPES"). In late October, the Internet Architecture Board recommended conditions that should be met if work on OPES continues, and in so doing cited CDT's policy concerns and urged that they be addressed.

The OPES protocol would enable an intermediary (such as a cache operator) in the middle of an Internet communication to alter the content of the communication as it passed from sender to receiver (for example, to insert an advertisement or screen the content for viruses). Although there would certainly be beneficial uses of the proposed protocol, it raises serious policy concerns about data integrity and privacy.

In early August, after analyzing the OPES proposal and concerns that had been expressed about it, CDT submitted extensive comments to the Internet Engineering Steering Group, a governing committee of the Internet Engineering Task Force ("IETF"). Following those comments, we participated in discussions on the OPES mailing list with proponents of the protocol. The proponents advanced a number of changes that addressed some of our concerns. In follow-up comments, we suggested that the OPES protocol effort should be permitted to proceed, so long as strong privacy and data integrity protections could be incorporated into it.

Last month, after reviewing the OPES proposal and the concerns raised by CDT and others, the Internet Architecture Board ("IAB") released its advisory comments on OPES. The IAB considered many of the issues that CDT had raised and recommended that any OPES effort must include strong protections for data integrity and privacy. CDT will be participating in any further discussions on OPES.

CDT's original comments on OPES are at http://www.imc.org/ietf-openproxy/mail-archive/msg00828.html.

Our follow-up analysis is at http://www.imc.org/ietf-openproxy/mail-archive/msg00935.html.

The IAB's analysis of OPES can be found at http://www.ietf.org/internet-drafts/draft-iab-opes-00.txt.

The draft OPES charter can be found at http://www.ietf-opes.org.

---

(2) BACKGROUND ON INTERNET STANDARDS, TECHNOLOGY & POLICY PROJECT The OPES proposal highlights a broader issue.

The Internet has tremendous potential to promote free expression and individual liberty. But will future technologies maximize this potential? Or will new ways to use the Internet have hidden downsides, such as a reduction of privacy? Will the technical requirements of new Internet services require resources beyond what individuals or small organizations can afford?

Increasingly, technical decisions about the Internet and its development can have far-reaching policy consequences. Often these technical decisions are made with little public awareness or input. At the same time, lawmakers and public interest advocates often debate policies governing the Internet without adequately assessing their technical merit or impact, and without appreciating how public policies can affect or even harm the technical development of the Internet.

To address these concerns, CDT has created the Internet Standards, Technology & Policy Project. A multi-year effort, the project has two goals:

- promote public awareness of and, where appropriate, involvement in the standards-setting, technical governance, and industry bodies that make technical decisions for the Internet;
- build better communication among technologists, public interest advocates, and academic policy leaders working on issues with broad relevance to Internet policy.

To direct the Internet Standards, Technology & Policy Project, CDT has recruited John Morris. John combines both a technical background and a law degree. He was one of the lead trial lawyers in the Reno v. ACLU case that first defined the high level of legal protections that speech over the Internet merits.

---

(3) INCREASING PUBLIC INTEREST PARTICIPATION IN STANDARDS PROCESSES Decisions about Internet technical standards or network architecture are generally not made by government agencies, which are under legal requirements to solicit and respond to public comment. Instead, decisions are made by private sector technical standards groups, including among others:

- the World Wide Web Consortium (W3C):
- the Internet Engineering Task Force (IETF):
- the Internet Corporation for Assigned Names and Numbers (ICANN).

Historically, public interest organizations have not been involved in the decisions of these bodies. CDT seeks

to promote a greater understanding of and appreciation for the work of these standards groups among a broader community. CDT does not seek to change the focus of the standards bodies away from technical decision-making, or to slow their decision-making processes.

As a critical first step in this process, CDT itself is now directly participating in the activities of the key standards bodies.

- Within the IETF, in addition to OPES, we are actively participating in the "geopriv" working group that has been tasked to develop technologies to protect privacy in geographic location-based services.
- Within the W3C (of which CDT is a member), CDT is actively engaged in the debate about the patenting of protocol technology and the issue of "royalty free" versus "reasonable and non-discriminatory" licensing of patented technology.
- CDT is active in a wide range of issues within the ICANN processes.

To broaden awareness and participation, we are planning a web site that will report on the work of the leading standards bodies and explain what issues are being addressed by the standards bodies and what policy concerns they raise. Through this web site, CDT hopes to give policymakers and public interest advocates an understandable window into the work of the standards bodies.

Further, CDT plans to work with a small network of technologists who can follow the work of standards bodies and explain emerging standards issues in non-technical terms.

---

(4) CDT SEEKS INPUT ON PUBLIC POLICY ISSUES ARISING IN THE STANDARDS CONTEXT A major challenge facing CDT's Internet Standards, Technology & Policy Project is how to track the activities of the many different relevant standards bodies and identify the potential public policy impacts that new and proposed standards could have.

In this effort, CDT welcomes input from technologists active in Internet standards setting bodies about activities and working groups that are likely to have significant impact on civil liberties, privacy, or other public policy concerns. Although we likely cannot pursue all issues raised to us, receiving advance notice of emerging policy issues will be critical to the success of the Project.

Input can be sent to the Project Director, John Morris, at jmorris@cdt.org.

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

CDT POLICY POST
Volume 7, Number 14, November 29, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) DOMAIN NAMES BODY REAFFIRMS PUBLIC ROLE, WITHOUT DETAILS The directors of the body responsible for technical management of the Internet domain name system committed to holding elections for public representatives, but left important implementation questions unresolved. In a resolution adopted at its meeting in Los Angeles, the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN) also refrained from implementing the controversial recommendations of a committee it had tasked to examine public representation. With these actions, the Board effectively deferred making major decisions on its own governance structure until its next public meeting in March, 2002, in Accra, Ghana.

ICANN coordinates critical elements of the Internet's infrastructure, including the naming and addressing systems on which online communications rely. Since its inception in 1998, ICANN has faced criticism for perceived shortcomings in representing the public interest. Presently, nine of nineteen seats on the ICANN Board of Directors are designated for "At-Large" Directors, to be chosen by the Internet user community -- although only five have actually been elected by users.

In November 2000, ICANN created an At-Large Study Committee (ALSC) to make recommendations on the question of public participation for ICANN. The ALSC's final report, released in early November 2001, supported the concept of user participation in ICANN, but several of its recommendations would have limited ICANN's inclusiveness and the voice of the user community. CDT and others questioned the report's practicality and fairness. In particular, the ALSC recommended that voting rights in future ICANN elections be restricted to those owning domain names and that public representation on the Board be limited to just six of nineteen Directors (as opposed to the current nine).

CDT opposed both of these limitations and joined an international coalition to provide workable alternatives.

The report of that coalition, the NGO and Academic ICANN Study, is available at http://www.naisproject.org/.

At its Marina del Rey meeting earlier this month, the ICANN Board accepted the ALSC document as a basis for further discussion, but importantly declined to adopt the ALSC's questionable recommendations.

The Board also re-committed itself to a short timeline for resolving representation issues. The terms of the five At-Large Directors publicly elected by Internet users in 2000 are set to expire in November 2002, and there are currently no provisions for their replacement. The Board resolved to begin planning election systems, and declared once again that the selection of new At-Large Directors should take place by November of next year.

More information on ICANN and on CDT's other activities in the area of domain names management can be found at http://www.cdt.org/dns/.

---

(2) ICANN BOARD ACKNOWLEDGES NEED FOR CONSTRAINED SCOPE OF ACTIVITIES In Marina del Rey, the ICANN Board took a first step towards acknowledging a need to place limits on the scope of its own activities. As part of a resolution establishing a Committee on Restructuring (see below), the ICANN Board noted that "it would be useful... to reaffirm and clarify ICANN's limited mission for technical management and administration."

Throughout its short history, ICANN has run the risk that it would make policy affecting the Internet without adequate processes to guide those policies. CDT and others have warned against the possibility of "mission creep," the likelihood that ICANN's authority over key resources could tempt it to enter policy areas it was never designed to handle. Already there has been some evidence that ICANN's activities are not sufficiently limited; many observers believe that the contracting process undertaken after last year's selection of new global Top-Level Domains (gTLDs) was fraught with questions about ICANN's appropriate policy role.

CDT believes that, in order to retain its legitimacy and protect the best interests of the Internet, ICANN should take every possible step to limit its likelihood of becoming entangled in inappropriate policy decisions. A clear restatement of ICANN's mission -- and, conversely, of areas not in ICANN's mission -- is necessary.

---

(3) INTERNAL RESTRUCTURING PLACED ON ICANN'S AGENDA As the issue of public representation in ICANN has continued to gain traction, other stakeholders have begun to complain of deficiencies in the ICANN process. Particularly within ICANN's most diverse stakeholder group, the Domain Name Supporting Organization, there have been long-running debates about the relative representation of various interests, and about the efficiency of the DNSO process in general.

This has led to a call for ICANN to revisit its internal structures. In Marina del Rey, the Board responded by establishing a committee of Board members to examine the issue and to report back to the Board at future meetings.

CDT believes that ICANN's internal structure should accurately reflect the wide range of interests affected by ICANN's activities. We look forward to working with ICANN on this issue, and hope that the committee will utilize an open, transparent process that includes the input of many throughout the Internet community.

---

(4) MEETING ADDRESSES ISSUES OF DNS, IP ADDRESS SECURITY With the events of September 11 in mind, much of the Marina del Rey meeting agenda consisted of panel discussions and roundtable meetings on improving the security of the systems under ICANN's administration. Attendees heard from speakers such as security experts Steve Bellovin and Bruce Schneier, U.S. government official John Tritak of the Critical Infrastructure Assurance Office, and Japanese Senior Vice Minister for Public Management, Home Affairs, Posts and Telecommunications Kenji Kosaka.

Notes of ICANN's real-time scribe and RealVideo archives of the speakers and roundtables are available at http://cyber.law.harvard.edu/icann/mdr2001/archive/.

CDT recognizes that security constitutes a core part of ICANN's mission. However, as ICANN continues its work in this area, we urge it to remain mindful of the fact that Internet security is an extremely broad area of which ICANN plays a small, though important, part. As it has already recognized, ICANN cannot and should not use its authority to promote security beyond the systems it manages.

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

CDT POLICY POST
Volume 7, Number 15, November 29, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

[Editor's Note: We appreciate that this is our second Policy Post today. Although we do try to limit the frequency of Posts, the following is a late breaking report and we did not want to delay it.]

Yesterday, November 28, the U.S. Supreme Court heard oral arguments in the most important Internet free speech case since the landmark ruling in the CDA case in 1997. Although the arguments yesterday raised challenging legal issues, CDT remains confident that in the final analysis, the courts will act to protect free speech on the Internet.

---

(1) U.S. SUPREME COURT HEARS ORAL ARGUMENTS IN THE ASHCROFT V. ACLU CHALLENGE TO COPA This week, the United States Supreme Court heard oral arguments in a major test of free speech online. In the case of Ashcroft versus ACLU, the Court is reviewing the constitutionality of the 1998 Child Online Protection Act (COPA). COPA imposes criminal and civil sanctions on any person who uses the Web to display "material that is harmful to minors" to anyone under the age of 17. Two lower courts - the federal district court in Philadelphia and the federal court of appeals - prohibited enforcement of COPA because it violates the First Amendment.

CDT, along with a broad coalition of publishers and public interest groups, filed briefs to the court of appeals and the Supreme Court arguing that COPA is unconstitutional. CDT also was counsel on a brief to the Supreme Court filed on behalf of leading Internet industry groups in support of the challenge to COPA.

The COPA statute is the successor to the Communications Decency Act (CDA) that was struck down in a pair of landmark lawsuits brought by CDT and others in 1996. In the CDA litigation, the Supreme Court held for the first time that speech on the Internet deserves the highest level of constitutional protection under the

First Amendment. In passing the COPA law after the CDA was overturned, Congress created a nearly identical scheme of government censorship that suffers from the same constitutional deficiencies that the courts found in the CDA. The ACLU and others challenged COPA in district court in Philadelphia. That court held that COPA is unconstitutional because it is not the "least restrictive means" to protect children on the Internet, and because it inhibits the publication of lawful speech to adults.

On appeal, the Third Circuit Court of Appeals agreed that COPA is unconstitutional, but relied on a legal analysis that had not been addressed by the district court. The appeals court found that the COPA statute is defective because it applies a "community standards" test to the nationwide (indeed global) Internet. Based on the global nature of the Internet, the Third Circuit Court of Appeals struck down the COPA statute. Yesterday, the U.S. Supreme Court heard oral arguments in the government's appeal of that decision.

CDT believes the Supreme Court argument continued to vindicate our belief that COPA is unconstitutional and suffers from the same flaws as the CDA. However, the argument left the suggestion that COPA may undergo further legal review before final resolution.

More information about the Communications Decency Act can be found at http://www.cdt.org/speech/cda/.

More information about the Child Online Protection Act can be found at http://www.cdt.org/speech/copa/.

---

(2) SUPREME COURT FOCUSES ON THE "COMMUNITY STANDARD" ISSUE Signaling the importance of the case, the Solicitor General of the United States, Ted Olson, argued for the government. The ACLU was well represented by Ann Beeson, who has been involved in Internet free speech cases since the original CDA case in 1996.

The Supreme Court Justices indicated early in the oral argument that they would focus only on the "community standards" issue addressed by the Third Circuit Court of Appeals.

Under the community standards approach, the lawfulness of sexually oriented speech is evaluated on a locality by locality basis. Although such an approach makes sense with media like magazines and videotapes that are sold in local stores, it does not translate well to the Internet, where most Web content is available to everyone.

The government argued that COPA could be upheld if the Court construes the "community standards" test to be a national test as applied to the Internet. In other words, if Internet content were challenged in court as "harmful to minors," a jury would be asked to determine whether the content is offensive based on what the country as a whole would find offensive (as opposed to what the jury's local community would find offensive). Several Justices expressed doubt about the ability of a jury to apply such a "national standard." Justice Scalia, for example, asked the government: "What does someone raised his whole life in North Carolina know about Las Vegas?" Chief Justice Rehnquist asked if a hypothetical North Carolina jury would pay any attention to an out-of-town expert witness testifying that certain content was acceptable nationally.

In her argument, the ACLU's Ann Beeson drove home the point that a national standard as sought by the government would likely reduce speech on the Internet to a level acceptable in the most conservative jurisdiction in the country. In other words, a New York City based web site could not post content that would be fully lawful in New York City, if the content might be deemed to be "harmful to minors" by a jury located in a very conservative rural community.

Beeson also forcefully argued that no matter how the Court resolves the community standards question, the

COPA statute still is unconstitutional for the reasons found by the Philadelphia district court. Beeson explained that the evidence considered by the district court demonstrates that many web sites would lose a substantial percentage of their visitors if the web sites were forced to comply with the constraints imposed by COPA.

Beeson also emphasized that filters and other user-empowerment tools were shown to be more effective in protecting children than the COPA law itself. Justice Ginsberg had pressed the government's lawyer on this point, asking whether COPA was really a "futile" exercise in light of the availability of sexual content hosted on overseas web sites and therefore outside the reach of the law. Solicitor General Olson argued that Congress had a right to take some steps even if those steps would not be perfectly successful, but Olson failed to grapple with the evidence that the COPA would in fact have little or no value in protecting children. As CDT and others have argued since the CDA case in 1996, parental tools such as filtering devices remain the most effective way to protect kids on the Internet.

---

(3) CDT REMAINS CONFIDENT THAT COPA ULTIMATELY WILL NOT SURVIVE LEGAL SCRUTINY

Although questions raised by the Court in oral argument are not necessarily predictive of the outcome of the case, yesterday's proceedings strongly suggested that the Court is aware of the constitutional challenges to COPA beyond the community standards issue. No matter how the Supreme Court rules on the community standards question, we believe it will ultimately consider the other free speech arguments advanced by the ACLU, CDT, and others, and find COPA to be unconstitutional.

On the community standards issue, CDT is hopeful that the Supreme Court will re-affirm that it would be unconstitutional for a federal law to limit speech on the Internet to the level that acceptable in the most conservative community in our country. CDT remains confident that on the basis of other challenges to COPA - which were not the focus of yesterday's hearing - the Court will permanently overturn COPA.

CDT will of course continue to follow the developments closely. A decision by the Supreme Court in the current appeal could come in the first six months of 2002, but will almost certainly be issued by June, 2002.

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

CDT POLICY POST
Volume 7, Number 16, December 18, 2001

A BRIEFING ON PUBLIC POLICY ISSUES AFFECTING CIVIL LIBERTIES ONLINE
from THE CENTER FOR DEMOCRACY AND TECHNOLOGY

CONTENTS:

---

(1) PRIVACY AND CONSUMER GROUPS LAUNCH ONLINE RESOURCE CDT and other consumer groups have launched ConsumerPrivacyGuide.org at http://www.consumerprivacyguide.org, a new online resource providing consumers with tips and other information on how to take control of their personal information and better protect their privacy.

CDT and many others believe that effective privacy protection for consumers online will be built on three pillars: industry self regulation and best practices; privacy enhancing technologies ("privacy by design"); and government regulation and enforcement. All three of these depend on consumers having access to information about what their rights are and what user empowerment tools are available to them. The ConsumerPrivacyGuide is intended to fulfill this need - to tell consumers what options are currently available to them to protect their privacy by controlling the collection and use of personal information.

Joining CDT in creating and co-sponsoring the site are Common Cause, Consumer Action, Privacy Rights Clearinghouse, Call for Action and the National Consumers League. The list includes groups with years of experience providing direct service to consumers; they will promote the site through their outreach activities.

---

(2) PRIVACY TIPS AND OTHER PRACTICAL INFORMATION; TOOLKIT PLANNED FOR 2002 The site provides consumers with the essential information they need to protect themselves when using the Internet. The site is intended for Internet users of all levels of experience and all age groups. It presents information, how-to tips and resources in consumer-friendly, straightforward language, covering the following:

- A "how to" guide to protecting privacy, explaining
  - How to read a privacy policy

    - How to opt out
    - How to read your financial services privacy notice
- A list of things users can do to protect privacy online, including how to
    - Reject unnecessary cookies
    - Use anonymous remailers
    - Encrypt your email
    - Use anonymizers while browsing
- Frequently asked questions, including a primer on "cookies" and how to manage them
- Links to other available online resources, such as opt-out sites
- A glossary of Internet and privacy terms
- Information about children's privacy
- Background on existing privacy laws

While information about privacy can be found online already, the new site organizes it and serves as a central jumping off point for consumers wanting to delve deeper into specific issues. The sponsoring organizations decided to pool their efforts in order to make the privacy issue less confusing for consumers. Given the flexibility of the Net, the site can be updated regularly to respond to new technologies, new privacy threats and new privacy enhancing measures.

The next step in this collaborative effort will be the release of an online "Privacy Toolbox," expected to go live in early 2002. That site will serve as a resource for privacy enhancing technologies and online demonstrations, such as how to use features of Internet browsers to manage cookies.

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