CDT POLICY POST
Volume 8, Number 1, January 29, 2002

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

CONTENTS:

---

(1) FEDERAL TRADE COMMISSION PROPOSES NATIONAL "DO NOT CALL" LIST Americans have said over and over again that they want to be able to avoid telemarketing calls at home. Their concerns range from the simple inconvenience of being interrupted at dinner to issues of fraudulent calls. Some federal rules are already in place that limit the time calls can be made (8am to 9pm) and that prohibit telemarketers from lying or misrepresenting their products. Some states have gone further.

Even with these limits, consumers still get unwanted calls - sometimes several in a single evening.

The Federal Trade Commission (FTC) is now trying to change that. The Commission has issued proposed new rules for telemarketers. The most important idea the FTC is considering is the creation of a national "do not call" registry. This would be a list that consumers would use to say that they do not want to receive telemarketing calls. Some states have such lists, and some marketers have their own "do not call" lists, but there is no one single place where consumers can go to ask to be taken off all calling lists.

For more background see FTC's Proposed "Do Not Call" Registry Page -- http://www.ftc.gov/bcp/conline/edcams/donotcall/index.htm

---

(2) How to submit comments to FTC Before going forward with such a national "do not call" program, the FTC wants public input. The FTC's full proposal is long and written for lawyers, but the FTC allows email submissions from ordinary citizens. To make it easier for you to make your voice heard in Washington, CDT has broken down some of the issues raised by the Commission and created a special site where you can

learn about the issue and file your comments.

Here's how it works: When you follow this link -- http://www.cdt.org/action/donotcall/ftc.shtml -- you'll come to a page with six questions posed by the FTC, with a block for your comments. Answer any or all of these questions. When you are finished, click "send." We'll create an automatic header with the proper official's name and the docket number and send your comments on to the FTC.

As always, we advise against flames.

Note that the FTC's comment process is public, so your comments will become public record. A copy of your letter will also be sent to CDT so that we can make sure that your letter was received by FTC and to eventually compile the best comments. We won't disclose your name or email address without contacting you and getting your express permission, nor will we use your information for any other purpose.

Written comments will be accepted until March 29, 2002. A public forum on the rule changes will be held at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580, on June 5, 6, and 7, 2002, from 9:00 a.m. until 5:00 p.m.

---

(3) What you can do to stop telemarketing today It may be months before the FTC's rule becomes final. Meanwhile, CDT has helped create ConsumerPrivacyGuide.org -- http://www.consumerprivacyguide.org -- an online resource that includes advice on how to get off telemarketing and direct mail lists and other helpful tips on what you can do to protect your privacy.

In addition to CDT, ConsumerPrivacyGuide.Org is sponsored by Call for Action, Common Cause, Consumer Action, the National Consumers League, and Privacy Rights Clearinghouse.

In addition, CDT offers Operation Opt-Out, http://opt-out.cdt.org/ an online resource that helps consumers through the maze of sometimes confusing and hard-to-find opt-out mechanism offered by online and offline merchants and marketers.

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

CDT POLICY POST
Volume 8, Number 2, February 21, 2002

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

CONTENTS:

---

(1) CALL FOR BEST PRACTICES, CASES STUDIES AND PAPERS FOR E-GOV TOOLKIT CDT, in association with the World Bank's InfoDev Program, is looking for best practices, case studies and papers for inclusion in a toolkit to guide the evolution of electronic government in developing countries.

The toolkit is intended to be used by technology and policy leaders in the developing world to design their own e-government projects.

Procedure: Send in your success stories, models, guides, etc, through the online form at: http://www.cdt.org/egov/submissions.shtml. Submissions for this toolkit must be of practical value. We ask that you designate your submission as either a best practice/case example or an overview/paper.

- Best practices and case examples should highlight how e-gov principles have been applied to specific projects in the developing world. We are looking for examples that provide good models for developing countries to follow.
- Overviews and papers should provide generalized guidance to those who are embarking on e-government, providing advance warnings of the pitfalls but also highlighting the opportunities and cost savings available. We are looking for papers that include accountability as part of the the e-government framework.

Submission deadline: March 31, 2002

Questions about the project, submission process, or outline should be sent to egovernment@cdt.org.

[Submissions sent to this address will be accepted, but we would prefer you to use the Web submission system].

---

(2) THE CONCEPT AND TOOLS OF E-GOVERNMENT E-government is the application of information and communication technology to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges within government, between governments and government agencies at federal, municipal and local levels, citizens and businesses; and to empower citizens through access and use of information.

There are three phases of E-Government:

- The "PUBLISH" phase -- tools that facilitate broader access to government information using information and communications technologies.
- The "INTERACT" phase -- tools that promote broader public involvement in participatory government.
- The "TRANSACT" phase -- tools that make government services available using information and communication technologies.

---

(3) THE ELEMENTS OF EFFECTIVE E-GOVERNMENT E-government is much more than creating government Web sites. In planning for the E-gov toolkit, CDT assembled an international advisory board who identified a set of key issues that must be addressed in order to make e-government successful.

- Process development: Critical to the success of e-government transformation is the understanding that e-government is not just about the automation of existing process and inefficiencies. Conversely, it is about the creation of new processes and new relationships between governed and governor.
- Leadership: In order to manage this change, leaders who understand technology and policy goals will be needed at all levels through government, from elected through to administrative levels.
- Strategic investment: Governments will need to prioritize some programs over others to maximize available funds in view of tightly limited resources. This will necessitate a clear objective for programs and a clear route to that objective.
- Public policy and law: New technologies have already thrown up a minefield of legal and policy questions. If e-government and e-commerce are to be successful, legislatures must be wary of short-term solutions. They must also take proactive steps to ensure that good intentions are backed up with policy commitment.
- Collaboration: Governments will have to explore new relationships with the private sector and NGOs to ensure quality and delivery of government services. Some agencies may also have to overcome traditional reluctance to work with each other to maximize benefits of scale in e-government projects.
- Civic engagement: E-government initiatives depend, to some extent, on an engaged citizenry and to that end, efforts to foster civic engagement are critical to the success of e-government plans.

---

(4) THE CHALLENGES AND OPPORTUNITIES OF E-GOVERNMENT The process e-government tools and systems often means facing new kinds of challenges. Developing countries, in particular, have many

barriers to overcome. Confronting these challenges directly can be a means to turn these difficulties into new opportunities. Our e-government toolkit is looking for responses to the following concerns:

- **Development**: All countries implementing e-government have struggled to develop a basic infrastructure to take advantage of new technologies and communications tools. This often includes problems of literacy and e-literacy.
- **Accessibility**: Governments must serve all members of society irrespective of their physical capabilities. In many countries more than one language or dialect will be prevalent -- setting appropriate standards for accessibility will be difficult. New services will have to be designed with appropriate interfaces -- this may have significant cost implications. The "digital divide" and disability issues are also continuing accessibility concerns.
- **Privacy**: Privacy is one of the fastest growing issue internationally. Governments are entrusted with huge amounts of personal information and must be a responsible custodian.
- **Security**: Security is costly but security breaches shatter public trust in government.
- **Transparency**: Government must be transparent in different ways to the private sector. This will be reflected in their choice and designs of ICT systems.
- **Interoperability**: Adding new systems on top of outmoded and legacy systems has been problematic for the private sector and will, in all likelihood, be problematic for the government sector.
- **Records management**: New technologies are being created to help manage information. Governments have unique needs in this field. Historical documentation is of special importance for governments.
- **Education and marketing**: E-government services are only useful if people know about them. Education and outreach programs will be needed. As the boundaries of the state become blurrier, new rules may be needed to govern the relationship of the public and private sectors.
- **Public/private competition/collaboration**: Issues of public vs private collaboration and competition are already part of an international debate on governance. E-government steps into a difficult area.
- **Intergovernmentalism**: Transforming government means individuals should be served by the easiest and most efficient means possible. But, this could raise serious constitutional and political issues about the relationship between states/provinces, federal government, (where applicable) local government, and the international community.
- **Workforce issues**: Human resources planning needs to be structured with the new goals in mind.
- **Cost structures**: Investment now, savings later. But planning and budgeting in an unstable climate is difficult.

We are planning to compile the toolkit in online, CD and printed versions, with indexing and searching capabilities that allow best practices and other materials to be correlated to the foregoing issues.

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

CDT POLICY POST
Volume 8, Number 3, February 25, 2002

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

CONTENTS:

---

(1) HOUSE COMMITTEE TAKES UP NEW CYBER-SECURITY BILL Months after making major changes to the surveillance and computer crime laws, Congress is considering a number of new bills dealing with cyber-crime, cyber-security, and surveillance. On February 12, 2002, the House Subcommittee on Crime held a hearing on H.R. 3482, the Cyber Security Enhancement Act of 2001. CDT Associate Director Alan Davidson testified.

CDT's testimony focused on Section 102 of the bill, which would greatly expand the authority of ISP's to disclose email and other Internet communications to the government in emergency situations.

Current law allows service providers to disclose their customers' email to law enforcement agencies without a court order if the ISP reasonably believes there is an imminent threat of death or serious injury.

Sec. 102 would substantially expand this authority to reveal private communications, by permitting service providers to disclose communications to any government agency (state, local or foreign) without judicial authority or oversight, where the threat is not immediate and where the ISP does not have any factual basis for its belief that there is an emergency other than the government's claim that there is one.

CDT's full testimony before the House Subcommittee on Crime is online at:
http://www.cdt.org/testimony/020212davidson.shtml

---

(2) EMERGENCY DISCLOSURE AUTHORITY RAISES PRIVACY, ACCOUNTABILITY CONCERNS

Under the USA PATRIOT Act adopted last fall, the communications privacy law was amended to allow ISPs and other system operators (universities, portals, Web hosts) to disclose the private communications of their subscribers or users if the system operator had reason to believe that there was an emergency situation involving an immediate danger of death or serious injury. The exception to the general rule of communications privacy was meant to cover situations where ISPs or others inadvertently discovered communications suggesting an immediate threat.

In fact, reports from large and small providers, universities, and libraries indicate that the provision is not being implemented as originally expected. Instead, providers are being approached by government agents and asked to voluntarily disclose communications or other subscriber information for investigations that the government claims involve a danger to life and limb.

Understandably, many service providers comply with the requests. But there is no oversight of these disclosures - they are not treated as interceptions, so they are not reported to the courts or Congress; the persons whose communications are disclosed are never given notice, even after the investigation is closed (unless, of course, the information is used in court); and service providers are immune (appropriately) from liability for disclosure. Furthermore, the exception doesn't even say that the disclosure must be limited to the communications to or from a suspected terrorist or other criminal - as written, anyone's communications can be disclosed in an emergency.

Section 102 of H.R. 3482 would expand this already broad authority:

- It would allow disclosures to any governmental entity, not just law enforcement agents. That could include literally thousands of federal, state, and local employees.
- It would not require imminent danger for disclosure. It would allow these extraordinary disclosures when there is some danger, which might be considerably in the future and far more hypothetical.
- It no longer requires a reasonable belief that there is a danger on the part of the ISP. Section 102 would allow these sensitive disclosures if there is any good faith belief of danger.

Thus as drafted, Sec. 102 would allow many more disclosures of sensitive communications without any court oversight or notice to subscribers. It would allow these disclosures based on requests from potentially hundreds of thousands of government employees, ranging from local canine control officials to school principals to Agriculture Department cotton inspectors.

CDT believes that the broad expansion would go too far. We urged the committee to maintain the requirements of a reasonable belief in imminent danger. We called for including accountability mechanisms - requiring notice to the subscriber, after the fact (and deferrable based on a judicial order), as a means of providing subscribers with some way of knowing that their communications have been disclosed. And at a bare minimum, we said Congress should mandate a reporting requirement for these emergency disclosures to federal law enforcement, to give Congress and the public some method of evaluating their use.

---

(3) STRONGER PRIVACY PROTECTIONS NEEDED ON OTHER POWERS TOO H.R. 3482 opens the door on an issue shoved aside by September 11: the need to improve privacy safeguards for a range of government surveillance activities. The digital age is making more personal information available than ever before, increasing the need for a legislative framework that protects personal information from inappropriate surveillance. The USA Patriot Act passed last fall provided substantial new government capabilities to conduct surveillance on Americans and to combat terrorism and cybercrime. H.R. 3482 would provides additional authorities. Powerful new surveillance authorities require powerful oversight and accountability. It is

time for equally strong measures for oversight and accountability, and protection for all the sensitive personal information increasingly available in the digital and wireless age.

Congress could start by taking up the privacy changes to surveillance law developed and passed by the House Judiciary Committee in the last Congress, in H.R. 5018, including:

- Heightened protections for access to wireless location information, requiring a judge to find probable cause to believe that a crime has been or is being committed before the government can use someone's cell phone as a tracking device. Tens of millions of Americans are carrying (or driving) mobile devices that could be used to track their movements over time - with little clarity over how that information could be accessed and without an appropriate legal standard for doing so.
- An increased standard for use of expanded pen registers and trap and trace capabilities, requiring a judge to at least find that specific and particular facts reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct.
- A rule prohibiting the government from using in court email or other Internet communications intercepted or seized in violation of the privacy standards in the law.
- Compilation of statistical reports for government access to email, similar to those required for telephone wiretaps.

In addition, other issues - some of broader scope - need to be addressed:

- Improve the notice requirement under ECPA to ensure that consumers receive notice (after an investigation is closed) if the government obtains information about their Internet transactions.
- Provide enhanced protection for personal information on networks: probable cause for seizure without prior notice, and a meaningful opportunity to object for subpoena access.
- Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.

For more information on H.R. 5018, see http://www.cdt.org/publications/pp_6.17.shtml

An overview of government surveillance authority (pre-PATRIOT Act) is at http://www.cdt.org/wiretap/wiretap_overview.html

---

CDT POLICY POST
Volume 8, Number 4, March 1, 2002

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

CONTENTS:

---

(1) ICANN PRESIDENT PROPOSES RADICAL CHANGES TO NET MANAGEMENT BODY M. Stuart Lynn, President of a key private management body for the Internet, has proposed a new structure for his organization that raises serious questions about whether principles of public accountability and openness will be applied in the administration of critical Internet resources.

Lynn is chief officer of the Internet Corporation for Assigned Names and Numbers (ICANN), the private non-profit body that coordinates certain important online domain name and addressing function -- such as the creation of new "top-level domains" like .com or .biz. The systems ICANN manages are global in nature, and CDT and others find ICANN's activities important enough that we have urged ICANN to provide means of participation for all affected interests.

The Lynn proposal provides an honest and forthright assessment of the problems facing ICANN. But its proposed remedies raise serious concerns. The Lynn proposal would scale back ICANN's accountability for its actions and its transparency before the online community. It would eliminate direct representation of users on ICANN's Board, replacing the nine members of ICANN's Board originally to be elected by the public "at-large" with five Board members selected by national governments. It would increase ICANN's budget 300-500% and seek funding from governments. It would change ICANN's relationships with the network operators it affects, requiring that they accept ICANN's authority and contribute financially in order to have a voice in its proceedings. Most important, it would do little to address core concerns about the unchecked growth of ICANN's powers and activities.

CDT harbors grave concerns about the Lynn proposal in its current form. We believe that the original conception of ICANN -- a non-governmental organization with a limited coordination function and committed to making sound technical decisions through open, bottom-up processes -- remains the best and most legitimate way to coordinate core Internet functions.

---

(2) ICANN REFORMS FAIL TO CONSTRAIN AUTHORITY, ACTIVITIES A top concern about ICANN is that what was once considered a narrow, "technical coordination" body could leverage its unique authority over Internet systems into much broader policy-setting activities - without adequate policy processes to ensure accountability to those affected by its decisions.

The Lynn proposal makes this problem worse, by reducing accountability while increasing the risk of "mission creep."

ICANN's central coordination role gives it the potential to exercise a great deal of power by conditioning how names and numbers are assigned. While the current ICANN Board admirably disavows any intent to set broader policies, a future Board will face tremendous pressure to use its authority to regulate the use of names, promote government taxation or consumer protection goals, or even control content.

There is already evidence that ICANN is exercising its powers beyond the minimal role set out in its founding documents. It has created massively detailed and regulatory contracts with the new top-level domains created in the last year. It exercised remarkable discretion in picking those seven new TLDs based on many factors besides technical merit -- including how names "sounded". It now turns its attention toward "keyword" systems that are not even part of the domain name system.

Unfortunately, the Lynn proposal fails to clarify ICANN's narrow, technical mission or to install safeguards that will prevent it from venturing beyond those prescribed limits. If anything, the proposal heightens the risk of "mission creep," most notably by seeking funding from governments and placing government-selected trustees on the ICANN Board. While governments have a role to play in the ICANN process, without clear guidelines such close ties to government will affect ICANN's independence and narrow mission.

CDT believes ICANN must get "back-to-basics" -- committing itself in a clear and tangible way to a core technical coordination mission, and providing checks and balances to ensure that its activities will remain limited. Without such a check on its authority, the user community will have difficulty ever trusting in ICANN.

---

(3) CDT, PARTNERS RESTATE PRINCIPLES FOR ICANN'S PUBLIC LEGITIMACY ICANN has worked hard to incorporate key principles of transparency, representation, and bottom-up governance. CDT and its international partnership to examine ICANN, the NGO and Academic ICANN Study (NAIS), are concerned that the Lynn proposal constitutes a disappointing retreat from these elemental principles. The proposal:

- Substantially diminishes ICANN's commitment to making its most important decisions in full public view;
- Creates a self-perpetuating structure, in which a substantial part of the Board would be chosen by the Board itself, rather than by stakeholder groups from the community;
- Reduces opportunities for meaningful participation by important sectors of the Internet community;
- Scales back the links of accountability between ICANN and the community of Internet users; and
- Centralizes ICANN policy authority at the top, with network operators expected to respond to ICANN rather than vice versa.

If ICANN abandons these principles, it risks becoming further detached from the interests of the community it was meant to serve. CDT and its NAIS partners strongly urge ICANN to keep these principles close in mind as it reviews the Lynn and other proposals.

The NAIS statement is available at http://www.naisproject.org/020301statement.shtml

---

(4) BOARD SHOULD CONTINUE ONGOING PROCESSES ON USER ROLE AT ICANN The Lynn proposal clearly merits attention, and will likely consume ICANN's attention for months to come. However, if the Board fails in Accra to pass bylaws preserving the At-Large Directors, then the outcome may be the same as if it took action to destroy them.

Dr. Lynn's publication of his reform proposal comes less than three weeks before ICANN's quarterly meeting in Accra, Ghana. At that meeting, the Board was expected to approve preparations for a new public election of five At-Large Directors. If preparations are not made, than an election will not take place this year and, as ICANN's current bylaws provide, the At-Large Directors will leave the Board without their replacements having been named. This would effectively terminate the role of the At-Large Membership at ICANN.

Moreover, the Lynn proposal has been released just as ICANN's own committee to examine the At-Large concept, the At-Large Study Committee (ALSC), is nearing completion of its work on reinvigorating the At-Large concept. Other groups, such as the NGO and Academic ICANN Study (NAIS), have made similarly large investments of time and energy in a process that is now being abridged.

The ICANN Board should not permit the introduction of this expansive new proposal to derail an ongoing process. In order to avoid prejudging the viability of the At-Large Membership, allowing all the effort so far expended to explore the public's role in ICANN to go to waste, the Board's Accra meeting should fully and openly treat the issue of At-Large membership before the Board moves on to new, more radical proposals.

- Dr. Lynn's proposal, "ICANN -- The Case For Reform," is available at http://www.icann.org/general/lynn-reform-proposal-24feb02.htm.
- CDT and its international partners, the NGO and Academic ICANN Study, released a major study in August 2001 entitled "ICANN, Legitimacy, and the Public Voice: Making Global Participation and Representation Work," available at http://www.naisproject.org/report/final/.

NAIS has also issued a more recent statement on the public voice in ICANN, "A Defining Moment for the At-Large and ICANN," available at http://www.naisproject.org/020222statement.pdf.

- ICANN's own At-Large Study Committee has published a number of documents with their own ideas about reforming ICANN. Available at http://www.atlargestudy.org/.
- Respected attorneys David Johnson and Susan Crawford most recently posted "ICANN 2.0," a new essay with their ideas about reforming ICANN. Available at http://www.icannwatch.org/essays/022602-johnson-crawford-icann2.htm.

For more information about ICANN and domain names management, visit http://www.cdt.org/dns/

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

CDT POLICY POST
Volume 8, Number 5, March 7, 2002

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

CONTENTS:

---

(1) CFP2002 IN SAN FRANCISCO: EARLY REGISTRATION DEADLINE IS MARCH 14 The Computers, Freedom and Privacy (CFP) conference is the pre-eminent forum for issues regarding democracy and technology. This year, it will be April 16-19 in San Francisco, California.

2002 marks CFP's 12th anniversary. As the Internet has grown, the conference has been able to maintain the collective and inclusive nature so elegantly chronicled in Bruce Sterling's book _Hacker Crackdown_. The CFP audience is as diverse as the Net itself, with attendees from the community of computer professionals, hackers, crackers and engineers who work the code of cyberspace as well as those from government, business, education, and non-profits grappling with the technology's public policy implications.

CFP is run on a non-profit basis under the auspices of the Association for Computing Machinery (ACM). All the planning work is done by volunteers - contributing to its wonderfully collaborative atmosphere.

March 14 is the deadline for early registration -- fees go up thereafter. Hotel discounts end on March 16.

For the schedule of events, general info and online registration, visit the CFP2002 site: http://www.cfp2002.org.

---

(2) SESSIONS ON LAW, PRIVACY, INTERNET GOVERNANCE, AND GLOBAL INTERNET POLICY ISSUES TO FEATURE CDT STAFF The program this year features many of the preeminent thinkers and policy makers in the field, including featured speakers such as California Attorney General Bill Lockyer, US Federal Trade Commission Chairman Timothy Muris, author James Bamford, John Perry Barlow, State Senator Jackie Speier, former Assistant Secretary of Commerce for Communications Larry Irving, and author

Bruce Sterling, among others.

CDT staff will be participating in many of this year's sessions:

- CDT's Executive Director Jerry Berman will be on a panel entitled "PATRIOT and Privacy" to discuss the implications of the USA PATRIOT Act on communications monitoring by law enforcement.
- Deputy Director James Dempsey will examine the various Internet policy challenges activists face around the globe and how those issues are being debated and regulated in a session called "Getting it Right: Global Internet Policy Issues."
- Associate Director Alan Davidson will moderate a panel on "ICANN in Year 3" to debate whether ICANN's promise as a bottom-up global self-governing Internet body is actually possible.
- CDT Staff Counsel John Morris will moderate a session on the open source movement and the standards process, which is expected to feature input from publisher and open source guru Tim O'Reilly.
- CDT Staff Counsel Paula Bruening will be on a panel exploring the current state of consumer education in the area commercial privacy, highlighting CDT's continuing work on http://www.ConsumerPrivacyGuide.com.
- CDT Policy Fellow Mike Godwin will teach both lawyers and non-lawyers about the basics of constitutional law and policy issues on the Internet in his always-popular tutorial "Constitutional Law in Cyberspace."
- Other sessions will take up such diverse issues as biometrics, national and international security, activism, privacy, and intellectual property.

CDT has taken an active role in CFP preparations, through in-kind sponsorship, membership on the conference's program committee, and most especially through the work of Assocaite Director Ari Schwartz, who serves as CFP 2002 Chair.

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

CDT POLICY POST
Volume 8, Number 6, April 5, 2002

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

CONTENTS:

---

(1) HOLLINGS INTRODUCES DIGITAL RIGHTS MANAGEMENT BILL Senate Commerce Committee Chairman Ernest "Fritz" Hollings (D-SC) introduced legislation March 21 that would require the consumer electronics and information technology industries to build standardized copyright protection technologies into computers, software and many other digital products. In CDT's view, such sweeping government mandates pose serious threats to innovation and the future of the Internet and digital technology in general as uniquely user-controlled, flexible, and open.

The announcement raised to a new level a long-running debate about how to protect intellectual property on the Net. Most recently, the debate has centered on the connection between putting copyrighted audio and video content on the broadband Internet and generating demand for broadband services. Right now, only about 10 percent of households that could get broadband have signed up for it. Although there are many explanations for this lack of consumer interest, many in the movie and music industries point to the lack of compelling content (movies and music) on the broadband Internet, which the content providers say they are holding back because of ineffective copyright protections. This reasoning -- and broader concerns about the ease of sharing big files over broadband -- has led to the proposal to legislatively mandate a scheme under which all technologies that might be used to play, copy, retrieve or transmit digital content -- whether on the Net or off it -- must be built so as to prevent illegal copying.

Sen. Hollings' bill, the "Consumer Broadband and Digital Television Promotion Act" (S. 2048), is co-sponsored by Sens. Stevens (R-AK), Inouye (D-HI), Breaux (D-LA), Nelson (D-FL) and Feinstein (D-CA). Under its central provisions:

- Makers of computers and consumer electronic devices, consumer groups and copyright owners would be encouraged to reach agreement on copyright protection standards and encoding rules.
- If the private sector failed to agree on standards within one year, the Federal Communications Commission would be required to develop them.
- All "digital media devices" -- TVs, audio and video players, and PCs, as well as many other devices -- would have to be manufactured to recognize and respond to those standards.
- The rules to be developed would have to preserve fair-use rights, including for educational and research purposes and legitimate consumer copying.

The Hollings bill is online at: http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s.02048:

---

(2) BACKGROUND ON THE COPYRIGHT PROTECTION ISSUE Some leading content companies see digital technology, with its capability for making 100-percent accurate, high-quality copies of digital data, as a threat to their profitability, especially when digital tools are combined with the capabilities of the broadband Internet. Their fear is that, just as the music industry had to cope with widespread Internet-based swapping of music files, soon the movie industry may face widespread, unauthorized trading of movie and TV files and other kinds of rich multimedia content over broadband networks.

The response of these content companies is that there needs to be a multi-industry technical standard -- backed by legislation -- that can prevent digital technology from being used to facilitate infringement. The goal of Hollywood's approach is to prevent copyrighted content from being circulated on the Net outside their control. But critics of the approach say that it appears that the only measures that could do this require top-to-bottom rearchitecting of the digital world, requiring the labelling of all copyrighted content and a redesign of all digital devices to look for the labels and permit or deny copying accordingly.

Makers of computers and consumer electronic devices as well as some major software companies are opposed to government mandates. These companies are willing to develop digital-rights management (DRM) technologies that can be used to limit or prevent unauthorized copying, and to license those technologies to Hollywood, but they oppose any standard that would require them to redesign all their products to check whether the files that are being read, copied or transmitted are copyrighted works. They see it as a form of government licensing and they worry about the costs, about whether the technologies will have unforeseen consequences for the functioning of their products, and about how the standards will limit future innovation.

An often unheard side of the debate is the consumer perspective: will such DRM technologies permit ordinary use that most consumers believe is proper, such as copying CDs onto a laptop, making a favorite songs CD for the car, or using a snippet of copyrighted content in a home video?

---

(3) SENATE HEARINGS OUTLINE DEBATE, WITHOUT MIDDLE GROUND Two Senate hearings -- one on the last day of February and one on March 15 -- underscored the extent to which leaders in the information-technology industry and the entertainment industry are at odds over copy-protection schemes for content.

The first of the two Senate hearings was before Sen. Hollings' Senate Commerce Committee. The witnesses included Disney chief Michael Eisner, News Corp. head Peter Chernin, and Jack Valenti, chairman of the Motion Picture Association of American, who complained about current Internet-based copyright infringement. During the hearing, several Senators warned that if the IT industry does not make more of an effort to agree upon solutions to the content industry's concerns, then Congress will step in and compel the IT industry to do so through legislation. The claims of the IT companies that innovation is put at risk by the broad technology mandates sought by Hollywood were met with skepticism by Senators, some of whom echoed the claim by one witness that an "eighty-cent chip" might be all that's needed to bring a PC into compliance with the proposed Act.

The second hearing, a Senate Judiciary Committee event chaired by Sen. Patrick Leahy (D-VT), reflected a more cautious approach. Witnesses included Richard Parsons of AOL Time Warner (a company with one foot on the IT side and one on the content side) and Jonathan Taplin, the CEO of Intertainer (a company that streams licensed copyrighted content over the broadband Internet). While several Senators expressed concern about Internet piracy -- especially the scope of piracy over broadband services -- Chairman Leahy also raised questions about the technical difficulties of implementing the kind of solution that Hollywood wants. Both AOLTW and Intel stated a willingness to cooperate in developing technical solutions, but stressed their reservations about broad government mandates and a preference for market solutions.

However, AOLTW's Parsons also said that narrower, more targeted legislation might be necessary soon, especially with regard to the infringement problems posed by digital television broadcasts and by the fact that copyright-protection measures may be lost when digital TV signals are converted for display on analog television receivers.

The Judiciary Committee panel also included Joe Kraus, a founder of Excite.com and more recently of DigitalConsumer.org, a new public-interest group that has been formed to promote a "Consumer Technology Bill of Rights."

Statements and other materials from the Judiciary Committee hearing are online at http://judiciary.senate.gov/hearing.cfm?id=197.

Materials from the Commerce Committee hearing are at:
http://commerce.senate.gov/hearings/hearings0202.htm

---

(4) CDT'S VIEW: TECHNICAL REVIEW AND A BALANCED, MARKET-BASED SOLUTION NEEDED

There is wide-spread agreement that the broadband Internet poses serious risks and significant opportunities for the music and movie industries and other makers of copyrighted digital content. CDT agrees that copyrighted material should be protected against piracy online. There are First Amendment interests on both sides. Unwarranted copying, by denying creators and artists compensation for their work, could adversely affect the free flow of information on the Internet and end up diminishing the power of the Internet that allows anyone to be a publisher.

But we are opposed to legislation that would mandate technical standards or require that all computer hardware and software include copy protection technology. We believe there is a better approach through market-based solutions that protect both copyright holders and consumers.

And before anything should happen, we believe there needs to be a fuller exploration -- and education of policymakers, consumers and the affected industries -- as to the technical implications and risks of the schemes being proposed. Also needed is a much broader consensus as to what consumer uses are

permitted under current law and how those uses would be protected.

In this context, the Hollings legislation raises a host of issues, ranging from the appropriate scope of the "fair use doctrine" (which has always permitted consumers some latitude in making copies of copyrighted material for personal use) to the potential impact on technology innovation of a government mandate requiring that all new technology include a particular copy protection scheme.

Nevertheless, it seems clear that the hearings have brought into the mainstream the issue of whether the content companies' legitimate concern about infringement will require new mandates on technology companies to redesign their products. It is also clear that more narrowly crafted measures, such as those alluded to by AOL Time Warner's Parsons, are on the horizon.

---

(5) LEAHY URGES CAREFUL CONSIDERATION, SEEKS PUBLIC INPUT Sen. Leahy made clear at his committee's hearing that there is significant disagreement among legislators as to whether it's yet even appropriate for Congress to be considering mandating a copyright security standard, and the Senator further promised that no legislation of the sort that Sen. Hollings had circulated will emerge from Congress this year.

To accompany the March 14 hearing, the Judiciary Committee staff has set up a new webpage designed to keep interested parties, including individual citizens, informed about developments on the copyright/technology-policy front. In an important step for digital democracy, the webpage also solicits citizens' direct feedback.

CDT urges all Internet users to visit Sen. Leahy's site and express their views on this issue, which may do much to define the future shape and functions of the Internet.

The Leahy webpage can be found at http://judiciary.senate.gov/special/feature.cfm.

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

CDT POLICY POST
Volume 8, Number 7, April 9, 2002

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

CONTENTS:

As Congress returns from its Spring recess on April 8, it faces a wide array of proposed legislation affecting the Internet. The bills run the gamut: some would advance the goal of user empowerment while others pose threats to democratic principles of openness, user-control, and privacy. It is impossible to predict what will be enacted before Congress adjourns in the Fall for mid-term elections, but here is an overview of some of the measures that are receiving serious consideration.

---

(1) CONSUMER PRIVACY LEGISLATION PROMISED Last Fall, Reps. Cliff Stearns (R-FL), Rick Boucher (D-VA), Bob Goodlatte (R-VA), and Billy Tauzin (R-LA) issued an outline of legislation to protect consumer privacy online and offline. Under their framework, companies would be required to give consumers notice of what information is collected about them and how it is used, and the ability to opt out of having their data shared with unaffiliated third parties. Companies could comply by following industry self-regulatory guidelines approved by the Federal Trade Commission (FTC). Under the proposal, consumers could not sue companies violating the law, but instead the FTC would be given power to enforce the rules. The proposal would preempt, or override, any state legislation that provided more protection for consumers' privacy. Rep. Tauzin, chairman of the House Commerce Committee, had said that legislation based on the outline would be issued

early in 2002, but nothing has been introduced yet.

Sen. Fritz Hollings, chairman of the Senate Commerce Committee, has also been drafting a consumer privacy bill. It is generally expected that the Hollings bill would be more far-reaching and in some respects more protective of consumer privacy than what the House Members outlined, but details have not been released.

The privacy outline of Reps. Stearns et al. is available at
http://www.house.gov/stearns/News-Views-Legislation/billoutlinedetail61.pdf

---

(2) COMPUTER CRIME AND COMPUTER SURVEILLANCE The House Judiciary Crime Subcommittee on February 26 reported a bill introduced by Chairman Lamar Smith (R-TX), H.R. 3482, the "Cybersecurity Enhancement Act." Sec. 102 of the bill would substantially expand the authority of ISPs and other companies to disclose private customer communications to the government without a court order anytime the service provider believes in good faith that there is an emergency posing a risk of death or serious bodily injury. Expanding an already broad emergency disclosure provision adopted last year in the PATRIOT Act, Sec. 102 has no checks and balances: no judicial review before or after the disclosure, no notice to the customer, and no statistical report to the Congress and the public on the number of disclosures and number of persons affected. CDT testified about its concerns regarding Sec. 102 and has been discussing them with staff for Chairman Smith and ranking Democrat Bobby Scott (D-VA).

Other provisions of the bill would: increase penalties for certain hacking and cybercrime offenses; require the Attorney General to establish at the FBI a National Infrastructure Protection Center to serve as a focal point for threat assessment, warning, investigation, and response to attacks on critical infrastructures, both physical and cyber; and establish within the Department of Justice an Office of Science and Technology to work on law enforcement technology issues, including investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

CDT's testimony on H.R. 3482 is at http://www.cdt.org/testimony/020212davidson.shtml

A link to the text of the legislation is at http://www.cdt.org/legislation/107th/wiretaps/

---

(3) HOLLINGS BILL WOULD MANDATE DIGITAL COPY PROTECTION On March 21, Senate Commerce Committee Chairman Hollings (D-SC) introduced legislation that would require the consumer electronics and information technology industries to build standardized digital rights protection technology into all their products. The "Consumer Broadband and Digital Television Promotion Act " (S. 2048) would require the electronics and IT industries, content providers and consumers to develop copyright protection standards and encoding rules within one year to be incorporated in all "digital media devices." TVs, audio players, and PCs would have to be manufactured to recognize and respond to those standards. The rules to be developed would have to preserve fair-use rights for educational and research purposes and legitimate consumer copying. If the private sector failed to come up with standards, S. 2048 would require the Federal Communications Commission to develop them.

In CDT's view, copyrighted material should be protected against piracy online, but sweeping government technology mandates pose serious threats to innovation and the future of the Internet and digital technology in general as uniquely user-controlled, flexible, and open.

The Hollings bill is online at: http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s.02048:

---

(4) HOUSE BILL CALLS FOR SPECIAL KIDS INTERNET DOMAIN NAME A House subcommittee on March 6 approved a bill mandating the creation of a new Internet domain aimed at protecting children online, ".kids.us." The bill directs the registrar for the ".us" domain name to create the new space. The bill would require that the operator of ".us" limit content in ".kids.us" to that which is "suitable" for minors under the age of 13. CDT has raised questions about the feasibility, effectiveness and constitutionality of a legislatively-mandated .kids domain. It remains far from clear that national standards of child appropriateness could be established. The process of creating and policing such standards risks running afoul of free speech protections.

Text of H.R. 3883, the "Dot Kids Implementation and Efficiency Act of 2002"
http://thomas.loc.gov/cgi-bin/bdquery/z?d107:hr3833:

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

Additional information on domain name related issues is available at http://www.cdt.org/dns/

- Both the Commerce and Judiciary Committees in the House have reported H.R. 718, the Anti-Spamming Act of 2001, sponsored by Rep. Heather Wilson (R-NM). The bill would amend the Federal criminal code to provide criminal penalties for intentionally transmitting ten or more unsolicited commercial email messages to one or more protected computers in the United States, with the knowledge that such messages are accompanied by or contain materially false or misleading information as to the identity of the initiator. The two Committees reported differing versions of the bill, which has delayed consideration by the full House. The bill as reported by the Commerce Committee contains a provision making it unlawful for a person to send unsolicited commercial e-mail to any recipient within the United States using the equipment of an ISP that has a policy against sending spam to its customers.

H.R. 718 also directs the Attorney General to prescribe labels to be included in e-mail that contains a sexually oriented advertisement in order to inform the recipient of such fact.

- H.R. 1017, the "Anti-Spamming Act of 2001," sponsored by Rep. Bob Goodlatte (D-VA) amends the Federal criminal code to make it unlawful for anyone to intentionally and without authorization initiate the transmission of a bulk unsolicited e-mail to a protected computer with knowledge that such message falsifies an Internet domain or other identifier or sell or distribute any computer program that is designed to conceal the source or routing information of such e-mail. It also provides civil penalties such as attorneys' fees and other litigation costs as part of civil relief from such violations.
- In the Senate, a similar bill has been introduced by Sen. Conrad Burns (R-MT): the CAN SPAM Act of 2001 (S. 630). It would amend the Federal criminal law to subject to a fine or imprisonment anyone who transmits an unsolicited commercial electronic mail message containing fraudulent routing information accompanied by header information that is materially or intentionally false or misleading. It would also require that all unsolicited commercial e-mail include a clear label identifying the message as an advertisement or solicitation; notice of the opportunity to opt-out of receiving further messages from the sender; and a valid physical postal address of the sender. The bill confers enforcement powers on the

Federal Trade Commission, other Federal agencies, and the States. It permits treble damages in a civil action brought by a provider of Internet access service adversely affected by a violation of this Act.

Links to the text and legislative history of spam bills: http://www.cdt.org/legislation/107th/junkemail/

---

(6) E-GOVERMENT BILL MOVES IN SENATE The E-Government Act (S.803), a bill intended to fundamentally change the way the federal government uses information technology to interact with citizens, was unanimously approved on March 21 by the full Senate Governmental Affairs Committee. Introduced by Sens. Joseph Lieberman (D-CT) and Conrad Burns (R-MT), the bill has undergone revisions following extensive negotiations among the sponsors, the Committee and the Bush Administration. While certain controversial provisions, such as the creation of an appointed Federal Chief Information Officer, were dropped or revised, the sections on access to government information and privacy that CDT has supported remained in the bill. The bill would require the government, for the first time ever, to systematically plan its enormous expenditures for computer systems in ways that will make government information and services more accessible to ordinary citizens, while also taking into account and mitigating the privacy implications of government data collection. CDT statement on e-government to the Governmental Affairs Committee, July 11, 2001 http://www.cdt.org/testimony/010711cdt.shtml

CDT press release in support of the E-Government Act, May 1, 2001
http://www.cdt.org/press/010501press.shtml

Links to the text of S. 803: http://www.cdt.org/legislation/107th/e-gov/

---

(7) FOIA EXEMPTION FOR INFORMATION ON COMPUTER AND INFRASTRUCTURE VULNERABILITY H.R. 2435, the Cybersecurity Information Act sponsored by Reps. Tom Davis (R-VA) and Jim Moran (D-VA), would create an exemption to the Freedom of Information Act (FOIA), requiring the government to withhold from the public "cyber security information" that is voluntarily provided to a Federal entity. Similar legislation in the Senate is S. 1456, sponsored by Sens. Bennett (R-UT) and Kyl (R-AZ).

The Davis-Moran bill defines "cyber security information" as information related to the ability of any protected system or critical infrastructure to resist intentional interference or incapacitation through the misuse of or unauthorized access to or use of the Internet, telecommunications systems, or other similar conduct that violates Federal, State, or international law, harms U.S. interstate commerce, or threatens public health or safety.

The Bennett-Kyl bill covers information about "any computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, ... or information or data in transmission or storage."

The bills also provide that cyber security information provided to the government could not be used by any Federal, State or local authority or by any third party in any civil action. The bills would also exempt private sector information sharing arrangements from the antitrust laws.

All pending legislation can be found at the Library of Congress web site http://thomas.loc.gov/

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

CDT POLICY POST
Volume 8, Number 8, April 23, 2002

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

CONTENTS:

---

(1) SEN. HOLLINGS INTRODUCES PRIVACY LEGISLATION In an important step toward instituting consumer privacy protection in federal law, Senator Ernest F. Hollings (D-SC) introduced on April 16 his long-awaited Online Personal Privacy Act, a bill to protect the privacy of individuals who use the Internet. CDT welcomes the introduction of the bill as reinvigorating the privacy debate and reaffirming that consumer privacy in the digital age remains a critical issue in the wake of September 11. CDT has consistently argued that, in addition to industry self-regulation and privacy enhancing technologies like the Platform for Privacy Preferences (P3P), federal legislation establishing workable and enforceable baseline standards is part of a comprehensive solution to the legitimate privacy concerns of Internet users.

Hollings chairs the Senate Commerce Committee, which will have jurisdiction over the bill. Co-sponsoring the bill are most of the Democrats on the Committee and two of its senior Republicans: Senators Breaux (D-LA), Burns (R-MT), Carnahan (D-MO), Cleland (D-GA), Inouye (D-HI), Kerry (D-MA), Nelson (D-FL), Rockefeller (D-WV) and Stevens (R-AK). The ranking Republican, Sen. John McCain (R-AZ), has refrained from co-sponsoring the legislation, but is believed to favor certain elements of the bill.

The Hollings bill is available in PDF at http://www.cdt.org/legislation/107th/privacy/oppa.pdf

---

(2) BILL INCLUDES FAIR INFORMATION PRACTICES; DISTINGUISHES BETWEEN SENSITIVE AND NON-SENSITIVE DATA The Hollings legislation incorporates the basic elements of fair information practices - long standing guidelines for collecting and handling information about individuals. The provisions of the bill include:

- Notice requirement: Sites must disclose the types of information collected, methods of collection, and use and disclosure practices.
- Consent requirements: Sites must provide users with an opportunity to consent to the collection, disclosure, or other use of information collected online.
- In the case of sensitive personally identifiable information - defined as health information, race or ethnicity, political party affiliation, religious belief, sexual orientation, Social Security Number and sensitive financial information - affirmative "opt-in" is required before such information can be collected, used or disclosed.
- To share non-sensitive personally identifiable information, sites must provide users with robust notice and opt-out consent.
- Access requirement: Sites must provide users with an opportunity to obtain reasonable access to information collected about them and to correct or delete information.
- State pre-emption: The legislation would pre-empt existing state law on privacy.
- Private right of action: Users would be afforded a the opportunity to bring suit and recover damages in state court against sites that collect, disclose or use sensitive personally identifiable information in violation of the legislation.

In addition, sites would be required to notify users upon making a change in their privacy policy, and could not change their information collection or use practices unless users have been given a chance to consent to the use of their information under the new policy. States would be empowered under the legislation to bring a civil action against sites to stop any practice in violation of the legislation, to enforce compliance and to obtain damages on behalf of residents of the state.

The bill only relates to online privacy - on the theory that the Internet poses unique issues of data collection and disclosure meriting separate treatment, it does not address data collection and sharing in offline contexts.

---

(3) HEARING SCHEDULED FOR APRIL 25, 2002 Several of the provisions, particularly the access requirements and the private right of action, are likely to meet with resistance from industry, while some privacy advocates are likely to argue that the bill does not go far enough. A hearing on the legislation is scheduled for April 25, 2002 before the Senate Commerce Committee. Witnesses expected to testify include Marc Rotenberg of EPIC, Frank Torres of Consumers Union, and representatives of Hewlett-Packard, Amazon.com, and the financial services industry.

For further resources about the consumer privacy debate, go to CDT's privacy page at http://www.cdt.org/privacy/

Links to other privacy legislation in Congress are at http://www.cdt.org/legislation/107th/privacy/

Information about how to better protect your privacy now is at the Consumer Privacy Guide, a resource created by CDT and other privacy and consumer advocates, http://www.consumerprivacyguide.org , and at the Privacy Toolbox: http://www.privacytoolbox.org

---

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

CDT POLICY POST
Volume 8, Number 9, April 26, 2002

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

CONTENTS:

---

(1) WEB PRIVACY STANDARD SET AS W3C RECOMMENDATION On April 16, the World Wide Web Consortium (W3C), the standard-setting body for the Web, issued the Platform for Privacy Preferences Project (P3P) 1.0 Specification as an official "Recommendation." The P3P 1.0 Specification is essentially a common language for expressing Web site privacy policies in machine-readable form. It allows users to set their Web browsers to automatically read Web site privacy policies and match them against a user's own preferences. Declaring P3P a W3C Recommendation indicates that it is a stable document, that it contributes to Web interoperability, and that the W3C Membership favor its widespread adoption.

P3P was designed by a Working Group composed of privacy advocates including CDT, Web technology leaders, data protection commissioners, and global ecommerce companies.

P3P alone will not resolve the privacy issue, but P3P is an important step in privacy protection because it can help consumers gain a better understanding of how Web sites collect and use their personal information. P3P-automated browsers allow users to easily view and understand privacy practices of the sites they visit. This awareness can empower users to control when, and to what extent, their personal information is released. Also, by giving consumers a standard way to compare practices across sites, this new transparency can help build a greater marketplace for privacy. The finalization of the standard should encourage Web sites and online businesses to build P3P into their sites. And the P3P vocabulary and P3P tools could also help regulatory and self-regulatory agents check for compliance with baseline standards.

The P3P Specification, the W3C announcement and a wealth of other information may be viewed at http://www.w3c.org/P3P/#news.

---

(2) BACKGROUND ON P3P Imagine walking down the street, looking into store windows. As you are about to enter a store, you see prominently displayed on the door an easy-to-read privacy policy that conforms to all local laws. Based on the notice you may decide to enter and shop or you may choose to take your business elsewhere. In this case, you choose to enter. After browsing the aisles, you select a product and head to the checkout counter. You hand over your credit card, cash or other form of payment and walk out with your purchase. The information you provided during the transaction will be used only for the purposes stated in the store's policy.

This is the P3P vision of online commerce. P3P is designed to provide Internet users with a clear understanding of how personal information will be used by a particular Web site, upfront, without having to read small-print legalese. Web site operators can use the P3P language to explain their privacy practices to visitors. Users can configure their browsers or other software tools to provide notifications about whether Web site privacy policies match their preferences. Parents can set privacy rules that govern their children's activities online. Consumers can make better judgments about which Web sites respect their privacy concerns.

P3P 1.0 creates the framework for machine-readable privacy policies. Web sites can express their privacy policies in a standardized format that can be read by Web browsers and other end-user software tools. These tools can display information about a site's privacy policy to end users and take actions based on a user's preferences. Such tools can notify users when the sites they visit have privacy policies matching their preferences and provide warnings when a mismatch occurs.

P3P is not a panacea for privacy, but it does represent an important opportunity to make progress in building greater privacy protections in the Web experience of the average user. There is still a strong need for additional privacy enhancing technologies; better consumer education; and baseline legislation to create a national standard for privacy expectations online. CDT strongly advocates the development of such initiatives, as well as the continued development of P3P.

For more information on P3P, see "P3P and Privacy: An Update for the Privacy Community," by CDT and the Ontario Information and Privacy Commissioner: http://www.cdt.org/privacy/pet/p3pprivacy.shtml.

The P3P home page is http://www.w3c.org/p3p/.

---

(3) INFORMATION ON ACCESS TO P3P TOOLS AND SITES There are several informative sites for consumers and businesses on P3P Implementation:

For an overview of P3P's history, FAQs and other background information on P3P and its derivation, the W3C provides an excellent resource at http://www.w3c.org/p3p/

Businesses interested in enabling their Web sites with P3P will find the necessary implementation guides at the P3P home page, http://www.w3c.org/p3p/. Other helpful assistance may be found at http://www.p3ptoolbox.org.

To assist in proper P3P implementation, the W3C has created a P3P policy validator, a tool that checks P3P policies to ensure no errors exist within the implementation code. The P3P policy validator is located at http://www.w3c.org/p3p/validator

For consumers and the general public, P3P-enabled Web browsers and plug-ins are available. These include Microsoft's Internet Explorer 6.0, which can be downloaded at

http://www.microsoft.com/windows/ie/downloads/default.asp and AT&T's Privacy Bird at http://www.privacybird.com. Netscape is expected to implement P3P in the Navigator browser in its next development cycle.

A complete implementation package has been created by the Joint Research Centre in Ispra, Italy -- http://p3p.jrc.it/index.php

Also, for an analytical background on P3P's development as a W3C Recommendation, its criticisms and rebuttals thereof, the P3P homepage provides documents and periodicals covering such issues: http://www.w3c.org/P3P/#papers

---

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

CDT POLICY POST
Volume 8, Number 10, May 10, 2002

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

CONTENTS:

---

(1) CDT URGES COURT TO BLOCK FRENCH NET CONTENT RESTRICTIONS IN US On May 6, CDT, the ACLU and other public interest groups filed a brief in the ongoing litigation to declare unenforceable a French court decision ordering Yahoo! to block French users from accessing a broad array of WWII and Nazi material. The French decision, requiring Yahoo! to change the architecture of its US-based services or face massive fines, has broad implications for free speech and commerce online.

The public interest groups filed their "friend-of-the-court brief" in the federal Court of Appeals for the Ninth Circuit (which includes California, where Yahoo! is headquartered). The brief argues that the French judgment represents an improper attempt by a foreign nation to apply its law beyond its borders to restrict expression protected by the constitution of the country where the creator of the content has its business operations -- in this case, the US Constitution.

The premise of the French court's ruling is a regime where web publishers in the US, the UK, Japan, or France itself could be held liable under the laws of hundreds of other countries based solely on the fact that a website can be viewed in those countries. Under such an approach, the brief argues, the burden of screening all content for all visitors against thousands of local laws would leave ISPs and content providers with no practical choice but to restrict their speech to the lowest common denominator of every country in the world in order to avoid liability - an outcome fundamentally incompatible with the value of free speech and the global nature of the Internet.

The brief argues that, in the United States, the French ruling would undermine First Amendment protection for Internet communications. We urged the appeals court to affirm a lower court decision holding the French ruling unenforceable in the US.

CDT's brief, the French Yahoo! decision (translated into English), and the lower US court ruling declaring it unenforceable can be found at http://www.cdt.org/jurisdiction/.

---

(2) CASE TESTS GLOBAL REACH OF NATIONAL COURTS The French court's order is but one example of the sort of judgment that courts around the world can expect to see with increasing frequency as Internet use expands globally. Given the borderless character of the Internet, controversial speech perfectly legal in one country is likely to be forbidden by laws somewhere else.

The May 6 brief lists some of the types of laws that regulate speech around the world, which could be used against web publishers if the regime contemplated in the French ruling is accepted. If French law can be enforced against California-based Yahoo!, then US-based websites - and websites around the world - might be faced with orders to block access to information that -

- "sabotages national unity," "goes against" the guiding principles of Communism, or "guides people in the wrong direction" in China;
- undermines "religious harmony and public morals" in Singapore;
- offends "the social, cultural, political, media, economic and religious values" of Saudi Arabia;
- constitutes "pro-Israeli speech" in the eyes of Syria;
- facilitates viewing of unrated or inappropriately rated websites in Australia; or
- constitutes information "offensive to public morality" in Italy.

These are just some of the types of restrictions that countries have applied to the Internet. The human rights implications of these restrictions are magnified if a country can issue civil or criminal judgments against offensive material created and hosted in another country where such material is perfectly legal.

Finding the French court ruling unenforceable in the US does not leave the French people without the ability to enforce their values within France. Under the position advocated by CDT in its brief, the kind of speech that the French ruling seeks to restrict in the US would still be illegal in France, and the French government could seek to prosecute those in France who produce it or access it . While CDT does not advocate such measures, countries have tools available to force ISPs within their own territory to block access to websites hosting disfavored content. Such approaches are far superior to making Internet publishers worldwide liable under foreign laws which they have no knowledge of or control over.

For CDT's July 2001 policy post detailing the rise in court decisions reaching content in other countries, go to http://www.cdt.org/publications/pp_7.06.shtml

---

(3) BACKGROUND: CHRONOLOGY OF THE YAHOO! CASE Here's the background on the French Yahoo! case:

- Nov 2000 - A French court ruled that Yahoo!, by allowing its US-based Web site to be accessed from France, violated France's law criminalizing the exhibition or sale of racist materials. The French court ordered Yahoo! to re-engineer its servers to identify French IP 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."
- Dec. 2000 - Yahoo! filed a lawsuit in the US federal court in its home district in California asking for a

declaratory judgment that the foreign verdict was unenforceable in the US. Yahoo! argued that the 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.

- June 2001 - The federal court in California denied a motion by the French defendants to dismiss the case.
- Nov 2001 - In a victory for Yahoo!, the federal court ruled that the French court's decision is unenforceable in this country because it requires a US company to censor material that is constitutionally protected.
- Dec 2001 - The private French groups that had initiated the case in France appealed to the Ninth Circuit Court of Appeals, claiming that the US district court lacked jurisdiction to determine whether the French court judgment is enforceable. In other words, after asserting broad jurisdiction of French courts over a US company operating in the US, the complainants asserted that US courts had no jurisdiction to determine whether the foreign order is enforceable in the US.
- May 6, 2002 - CDT, ACLU and others file brief in the Ninth Circuit Court of Appeals. The U.S. Chamber of Commerce and other leading Internet industry groups file a similar brief opposing the French court's ruling.

---

(4) INTERNET INDUSTRY ALSO FILES "FRIEND OF THE COURT" BRIEF SUPPORTING YAHOO! Also on May 6, a coalition of leading business organizations and associations -- led by the U.S. Chamber of Commerce -- filed a brief with the Court of Appeals in support of Yahoo!.

The industry brief is directly complementary to the arguments made in the public interest brief filed by CDT and others. Just as the decision of the French court is a serious threat to free speech, it is also a threat to companies' ability to do business on the Internet. The industry brief argues that the French court lacked jurisdiction (and thus was without power) to order a US company to change its US-based and US-focused web site based solely on the fact that the web site could be viewed in France. The brief also argues that the California federal district court did have the power to step in and declare that the French court order was unenforceable.

Taken together, the briefs filed by the public interest coalition and the industry groups strongly articulate the serious threats to speech and commerce on the Internet that are created when one country tries to censor the entire Internet.

The industry brief is also available at http://www.cdt.org/jurisdiction/

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

CDT POLICY POST
Volume 8, Number 11, May 13, 2002

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

CONTENTS:

---

(1) SUPREME COURT KEEPS INJUNCTION AGAINST COPA NET CONTENT CONTROLS The Supreme Court issued a ruling today in the case challenging the Child Online Protection Act (COPA), a federal law that restricts online content deemed "harmful to minors." Two lower courts had ruled that COPA violated the First Amendment and enjoined its enforcement. The Supreme Court today kept that injunction in force, blocking the Justice Department from enforcing the Act. The Court also returned the case to an intermediate-level appeals court based on flaws in that court's interpretation of the long-standing "community standards" obscenity test as applied to the Internet.

Major points about today's ruling:

- The Supreme Court did not say that COPA is constitutional. All nine Justices of the Court agreed that the lower court injunction against COPA should remain in effect pending further court proceedings.
- The Supreme Court was explicit in saying that its decision was a narrow decision that only addressed a specific conclusion of the Third Circuit Court of Appeals - namely, its holdings about community standards.
- Nothing in the Supreme Court decision casts doubt on the original holding of the U.S. District Court that COPA is unconstitutional.
- The Supreme Court did not give any indication of its views on the theories mainly relied upon by those challenging COPA, namely, that in the name of protecting children it would force Web publishers to take down material that is legal for adults and protected under the First Amendment.

In sum, nothing in today's ruling detracts from CDT's belief that COPA should ultimately be found unconstitutional, and suffers from the same fatal First Amendment flaws of its predecessor, the Communications Decency Act.

You can download the Supreme Court decision from http://www.cdt.org/speech/copa/020513opinion.pdf

Briefs and the text of COPA are online at http://www.cdt.org/speech/copa/

---

(2) "COMMUNITY STANDARDS" THEORY OF APPEALS COURT REJECTED The Child Online Protection Act, passed in 1998, makes it a crime for anyone, by means of the World Wide Web, to make any communication for commercial purposes that is "harmful to minors" unless the person has somehow restricted access by minors (for example, by requiring a credit card number.) COPA imposes criminal and civil penalties of up to $50,000 per day for violations. CDT had long argued that COPA unconstitutionally burdens speech that is protected for adults. In 1999, a federal district court agreed and prohibited the Justice Department from enforcing of the statute. That ruling was appealed by the government, and upheld by the Third Circuit Court of Appeals in 2000.

The Third Circuit had based its decision on a theory that had not been advanced by any party - that the traditional "community standards" test for judging what is illegal obscenity could never apply to the Internet. The Supreme Court rejected that broad theory, but specifically did not address the grounds on which the District Court originally declared COPA unconstitutional.

While the court rejected the Third Circuit's conclusion that a "community standards" test could never apply to the Internet, it left the test open to further challenge in later litigations. Moreover, the Court left open a host of issues that would have to be resolved in applying community standards to the Internet. For example, different justices expressed different opinions about whether the "local" community standards of the country's most conservative communities would govern Internet content, or whether a new "nationwide" community standards should apply online.

As a practical matter, the primary result of the Supreme Court's decision is that the case will be remanded -- or sent back -- to the Third Circuit Court of Appeals for consideration of the First Amendment grounds on which the district court struck down COPA . The district court has already conducted a hearing and concluded that COPA restricts speech in a manner that violates the First Amendment.

Beyond that, it is hard to draw many conclusions from the Supreme Court's decision, for the Justices were highly fractured: Justice Thomas filed the "opinion of the Court," but only two other Justices (Chief Justice Rehnquist and Justice Scalia) agreed with everything Thomas wrote. Justices O'Connor and Breyer each filed solo opinions "concurring in the judgment" that the appeals court's reasoning was wrong. Justice Kennedy, Souter, and Ginsburg filed a different concurrence, and Justice Stevens filed a dissent.

---

(3) EDUCATION AND USER CONTROL, NOT LEGISLATION, KEY TO PROTECTING KIDS ONLINE The Supreme Court ruling highlights the difficulties in trying to legislatively control content on the Internet. In that respect, the Supreme Court decision echoed the findings last week of the National Research Council (NRC), which concluded after exhaustive study that legislation will not solve the problem of children's access to objectionable content via the Internet.

Even as Congress passed COPA, in separate legislation it directed the NRC to conduct a study about how best to protect children from inappropriate material online. That study has now conclusively demonstrated that legislation simply will not work to protect children. As the COPA case is sent back to the Third Circuit, the NRC study will be very relevant to the question whether COPA is the least restrictive means for protecting

children.

This expensive cycle of legislation and litigation does little to serve children and families online. CDT believes that giving users control over what they see and do online - through education and through tools such as those collected at sites like http://www.getnetwise.org - will more effectively protect kids in ways consistent with their own family values, and with the Constitution.

Instead of passing new laws - which do little to address the majority of adult content that is now overseas - the government can encourage and foster education for children and families about how to assure a safe online experience for children. In addition, it can devote increased resources for better enforcement of laws against child predation and child sexual exploitation.

The NRC study, "Youth, Pornography, and the Internet," is online at http://www.nap.edu/books/0309082749/html/

CDT POLICY POST
Volume 8, Number 12, May 16, 2002

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

CONTENTS:

---

(1) CAPITOL HILL "BUSY SEASON" BRINGS WAVE OF INTERNET PROPOSALS In both the Senate and the House of Representatives, a number of bills under active consideration have important consequences for civil liberties online. In this Policy Post, we summarize some of the most notable Internet-related legislation recently introduced in Congress and moving through its Committees.

For regularly updated information, see CDT's bill-tracking pages at http://www.cdt.org/legislation/.

---

(2) PRIVACY LEGISLATION APPROVED BY SENATE COMMITTEE On May 16, the Senate Commerce Committee marked-up S. 2201, the Online Privacy Protection Act, introduced by Senator Ernest Hollings (D-SC). "Marking up" a bill means amending it in a formal Committee session where Members or Senators offer amendments, debate them and vote on them. Often at mark-up many amendments are rolled into a single "substitute" offered by the bill's sponsor. That is what happened in the May 16 mark-up of S. 2201. Normally, a mark-up concludes with a vote to "report" the bill to the full House or Senate with a recommendation calling for its consideration and passage. That did not happen on May 16. Due to procedural maneuvering most Senators themselves did not fully understand, the Committee was barred from reporting the bill on the 16th.

As of this writing, the Committee was expected to meet at 9:30 on the morning of Friday, May 17 to finish its work and report out the bill as amended.

The Hollings bill addresses the collection, use and disclosure of personally identifiable information online, requiring --

- notice of data collection and use practices;
- opt-in consent for collection and sharing of sensitive personally identifiable information;
- opt-out for nonsensitive information;
- consumer access to information held about them.

The bill would pre-empt state law regulating Internet privacy, and would provide for a private right of action for persons whose sensitive information has not been treated in accordance with the bill's provisions.

The substitute approved on May 16 preserved all of these elements while making many changes designed to clarify the bill or assuage various concerns. Among other things, the substitute required some form of authentication for consumers to access their data held by businesses.

The Committee also approved three other amendments: one, offered by Sen. Brownback, establishes a "safe harbor" for small businesses; another, by Sen. Allen, makes it clear that the access provision does not require companies to disclose proprietary information; and the third, by Sen. Nelson, requires each covered entity to designate some employee responsible for compliance.

The Committee rejected an amendment offered by Sen. John McCain (R-AZ) that would have extended the bill to cover offline as well as online data collection. The McCain amendment was of concern because it would have broadened the bill without taking account of the differences between the online and offline worlds.

Instead, the substitute included language from Sen. Barbara Boxer (D-CA) that would require the Federal Trade Commission to write rules for the offline world within 6 months of the law's enactment and submit them to Congress for evaluation, with the rules taking effect 13 months after that unless Congress rejected them or adopted new ones. This approach would create an incentive for lawmakers to make general privacy protection a major issue for the next Congress.

The Committee also rejected amendments to remove the private right of action and to preempt state common law privacy rules (privacy rights established over many years in judicial decisions).

Several Senators indicated that they had additional concerns with the bill that they would raise with amendments offered when it reaches the full Senate.

The Hollings bill as introduced, CDT's analysis of it, and the text of the amendments adopted on May 16 are all available at http://www.cdt.org/legislation/107th/privacy/hollings.shtml.

---

(3) JUNK E-MAIL LIMITS GAINING MOMENTUM Also on May 17, the Senate Commerce Committee is scheduled to mark up S. 630, the "Controlling the Assault of Non-Solicited Pornography and Marketing" ("CAN-SPAM") Act. The measure, introduced by Sens. Conrad Burns (R-MT) and Ron Wyden (D-OR) , would impose various requirements on senders of commercial e-mail (also known as spam), some backed up by criminal penalties, others by civil fines enforced by the Federal Trade Commission or the state Attorneys General, and would authorize lawsuits by ISPs against spammers.

The latest version of the Burns-Wyden bill would:

- Define commercial e-mail as any message whose primary purpose is "the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."
- Make it a crime to send unsolicited commercial e-mail with header information that is materially false or misleading.
- Make it a civil offense to send any commercial e-mail with header information that is materially or intentionally false or misleading.
- Make it a civil offense to send any commercial e-mail with a deceptive subject heading.
- Require all unsolicited commercial e-mail to include a functioning return e-mail address that enables recipients to opt-out of future e-mail.
- Prohibit sending unsolicited commercial e-mail to those who have requested not to receive it.
- Require all unsolicited commercial email to include, in addition to an opt-out address, an "identification" that the message is an advertisement or solicitation and a valid physical postal address of the sender.

CDT believes that the general approach of the Burns-Wyden bill, while not a complete solution to the problem, represents a positive and constitutional response to one of the most irritating annoyances Internet users face. Requiring truthful header information, a valid return address, and opt-out in commercial speech are reasonable measures, and in our view they should be constitutional so long as they allow for anonymity. As we read the bill, it is not a violation of the bill's requirement to use an anonymous or pseudonymous email address, and we are urging Sens. Burns and Wyden to make that clear.

CDT is concerned, however, with three provisions:

- The "identification" requirement, which is a form of mandatory labeling and thus a form of compelled speech that is unconstitutional in the absence of a compelling governmental interest and a showing that it is narrowly tailored to serve that interest. It is also certain to be ineffective, since the bill does not specify the form or location of such identification - it could be buried in the text of a message - and thus is unlikely to be useful for end-user filtering of e-mail.
- The provision that would require truthfulness in the subject line of e-mail. This standard, especially as applied to advertising, seems so subjective that it would be arbitrarily applied and could chill normal commercial speech. There is already a law against deceptive advertising, backed up by decades of judicial interpretation; the bill, by seeming to create a new rule just for e-mail based advertising, could sow confusion, while adding no new protection to consumers.
- The requirement that all unsolicited commercial e-mail include a valid physical address for the sender could affect the right to anonymity and privacy, especially of small business owners or individuals engaged in commercial activity out of their homes.

In addition, we believe the definition of commercial e-mail could be further clarified to avoid sweeping in e-mail linking to websites whose primary purpose is not commercial.

The Senate Commerce Committee is expected to take up the spam bill when it reconvenes on Friday, May 17.

The Burns bill is available through Thomas at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s630:.

---

(4) BILLS WOULD LOOSEN STANDARDS ON GOVERNMENT ACCESS TO E-MAIL Provisions of two new bills -- one to increase online "cybersecurity," the other to aid in the prosecution of online child pornography -- would remove statutory protections that safeguard personal data in the hands of Internet Service Providers (ISPs).

Current law protects the privacy of electronic communications by prohibiting ISPs from disclosing to the government their customers' e-mail without a court order. The two new bills open loopholes in that protection by creating broad new categories of "voluntary" disclosure. If such disclosures are permitted, then the government could gain access to users' private information without receiving a judge's approval, and without notice to the users themselves.

- H.R. 3482, the "Cyber Security Enhancement Act," would lower the standard under which the government could gain access to e-mail in emergency situations. It would allow ISPs to disclose data without a court order whenever the ISP believes in good faith that there is an emergency involving risk of death or serious bodily injury to someone. This means that the government can come to an ISP, claim that there is an emergency, and the ISP, in good faith believing the government agents, can disclose the data.

The provision does not require that the government agents have to be acting in good faith. Nor under the new language, does the danger have to be immediate. There is no need to seek review by a judge, even after the emergency has passed, and there is no requirement to notify the customer that his email has been disclosed. There is no time limit on how many days or months of e-mail can be disclosed.

H.R. 3482 was marked up and reported by the House Judiciary Committee on May 8.

- H.R. 4623, the "Child Obscenity and Pornography Prevention Act," is intended to overturn the Supreme Court's April 16, 2002 decision on virtual child pornography, by making it a crime to produce, disseminate or possess computer-generated child pornography images that appear virtually indistinguishable from images produced with actual children.

However, the bill includes an unrelated provision that would make it easier for the government to read private e-mail. Currently, ISPs are required to disclose data without a court order, but only if a child pornography violation is "apparent," meaning if the ISP finds on its own child pornography images.

Under the new provision, disclosure would be permitted if the government informally tells an ISP that a violation "may have occurred or will occur." This dispensing with the court order requirement is not even limited to emergency situations where the government does not have time to get a court order. As with the disclosure that would be permitted under H.R.3482, the disclosure in child porn cases would not be subject to court review , nor would targets improperly investigated ever be notified of their ISPs' actions.

The text of the bills and related material can be found at http://www.cdt.org/legislation/107th/wiretaps/.

CDT's testimony on H.R. 3482: http://www.cdt.org/testimony/020212davidson.shtml.

---

(5) SEVERAL NEW BILLS INTRODUCED AFFECTING INTERNET DOMAIN NAMES In recent weeks, there has been a wave of activity concerning Internet domain names -- the addresses, such as www.cdt.org, used to identify resources on the Internet.

- H.R. 4640, introduced by Reps. Howard Coble (R-NC) and Howard Berman (D-CA), would make it a federal felony to provide, "with intent to defraud," misleading false contact information in registering for a domain name. Given the way the domain name registration system is currently operated, CDT is concerned that the bill would seriously jeopardize the privacy and free speech rights of Internet users.

The bill affects the database of domain name owners' names, addresses, telephone numbers, and e-mail addresses known as the Whois database. The Whois database is publicly accessible worldwide, and is a tool for law enforcement, copyright holders and others with legitimate interests in identifying the owners of domain names.

Although the Whois database has many legitimate uses, its managers have never found a way to balance the legitimate uses of the information against the risks to privacy and anonymity. For many individuals, registering a domain name for personal or political use means making a home address, home phone number and/or personal e-mail address publicly available in the Whois database.

Today, Whois is currently wide open to anyone for any purpose. This allows it to be used for undesirable activities ranging from spam and unwanted telemarketing to felony crimes. Since Whois currently offers no protection for individual users' privacy, some users have taken matters into their own hands by entering false or incomplete information into the Whois database. The Coble bill could make such actions a federal crime carrying up to five years in prison. CDT questions whether exposing millions of Internet registrants to such potential criminal liability is appropriate, especially without further clarification of the law and added privacy protections for personal and non-commercial domain names.

The House Judiciary Subcommittee on the Internet and Intellectual Property has scheduled a hearing on the Whois database of May 22.

- H.R. 3833, the "Dot Kids Implementation and Efficiency Act of 2002," would instruct the company administering the .us Internet domain to create a new .kids.us domain that would contain only material appropriate for children below the age of thirteen. Such a domain, however, is likely to be difficult and expensive to maintain, and may not provide significant protection for children. CDT remains wary of the "slippery slope" involved when applying content standards to the Internet.

H.R. 3833 was approved by the Commerce Committee on March 10 and awaits consideration by the full House of Representatives.

- S. 2137, the "Family Privacy and Security Act of 2002," introduced by Sen. Mary Landrieu (D-LA), would instruct ICANN -- the Internet Corporation for Assigned Names and Numbers, which administers the global domain name system -- to create a top-level Internet domain expressly for material "harmful to minors." The bill would require any commercial web site that has as its principal or primary business the making available of material that is "harmful to minors" to register in that domain.

CDT has grave reservations about this approach to protecting children online. Mandatory categorization of content is a form of forced speech raising serious constitutional concerns. The provision would enmesh the domain names industry, online publishers and courts in endless debates about what is and what is not harmful to minors. Moreover, it is hard to see how the proposal could be implemented on the global Internet where there is no international agreement on what is "harmful to minors."

CDT will continue to point out to legislators that passing new laws like this is not nearly as effective as non-legislative means of child protection such as education of parents and children, parental installation of filters, and school and library acceptable use policies.

Links to these bills are at http://www.cdt.org/legislation/107th/dns/.

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

CDT POLICY POST
Volume 8, Number 13, May 30, 2002

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

CONTENTS:

---

(1) CDT Project on Standards Explores Policy Impact of Technological Decisions Internet technical standards have a major impact on the Internet's uses and its future development, with broad implications for public policy and individual rights. For this reason, CDT launched last year its Internet Standards, Technology, and Policy Project, to increase public awareness of and input into technical decision-making. Our goal is to ensure that the Internet will continue to offer the freedom and empowerment users now enjoy.

To better serve the public interest community and bring a broader perspective to standards processes, CDT's Standards Project is taking two important initiatives:

First, we are expanding our Standards Project website, at http://www.cdt.org/standards/. This site will contain news and alerts about public policy issues in the standards world, background information on the leading standards bodies, and information on the Standards Project. Over the coming months, we hope that the web site evolves into a useful resource for both public interest advocates who are not Internet experts and for technologists interested in public policy aspects of standards development. We welcome your input on how to best facilitate an end-user voice in standards processes.

Second, we are launching a Standards Bulletin, which every six to eight weeks will provide updates and analysis about the work of the organizations that design the standards and make other important technical decisions for the Internet. Our goal is to provide the public interest community with an introduction to the standards world, identify and track emerging issues, and raise the public interest involvement in the often complex process of standards development.

In this issue of the CDT Policy Post, we are attaching issue number one of the Standards Bulletin. We hope you find it interesting, and look forward to your feedback!

If you would like to receive future issues of the Standards Bulletin, you can subscribe to it at the project website, http://www.cdt.org/standards/

---

(2) CDT Standards Bulletin 1.01 May 30, 2002 [Standards Bulletin 1.01 -- May 28, 2002 [
[Policy Updates and Analysis from the Internet Standards World
[Provided by
[The Center for Democracy & Technology's
[Internet Standards, Technology, and Policy Project

Welcome to the first issue of the Standards Bulletin, a new publication from CDT's Internet Standards, Technology, & Policy Project.

Internet technical standards have a major impact on the Internet's uses and its future development, with broad implications for public policy and individual activities. Public awareness of and input into technical decision-making are needed to ensure that the Internet in its future evolution will continue to offer the freedom and empowerment we now enjoy. Public policy makers and policy advocates need to be more familiar with the development of Internet standards and the issues they bring to the fore.

Every six to eight weeks, the Standards Bulletin will provide updates and analysis about the organizations that design those standards and make other important technical decisions for the Internet, such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). Our goal is to provide the public interest community with an introduction to the standards world, identify and track emerging issues, and raise familiarity with the often complex process of standards development.

Along with this Standards Bulletin, we are also pleased to be launching our Standards Project website, at http://www.cdt.org/standards/. This site contains news and alerts about public policy issues in the standards world, background information on the leading standards bodies, and information on the Standards Project. Over the coming months, we hope that the web site evolves into a very useful resource on public policy and the standards processes. We welcome any input from the community on these and other efforts to facilitate an end-user voice in standards development.

John B. Morris
Director, Internet Standards, Technology, and Policy Project of the Center for Democracy & Technology

---

1 - Standards Spotlight: IETF's GEOPRIV Working Group.

A new working group at the Internet Engineering Task Force (IETF) is addressing serious issues concerning the privacy of sensitive "location" information used in a variety of emerging technologies. As new technologies expand wireless access to the Internet, a huge array of location-based services are in the works. Along with consumer uses, such services can provide increased security and enhanced emergency services. There are also on-going projects aimed at providing (or in some cases limiting) services and content based on the location of users with stationary Internet access.

Significant privacy and security concerns are raised by these location-based services. Although many location-based services will be optional and fully user-controlled, in some cases users will have little choice but to reveal sensitive location information. Even with user-approved services, there is a significant need to protect and limit the dissemination of location information.

In mid-2001, in recognition of the serious privacy and security issues raised by location based services, the Internet Engineering Steering Group (IESG) of IETF decided to establish the "GEOPRIV" working group for the purpose of designing to protect the privacy of location information. As defined by its charter, the mission of the working group is to assess the authorization, integrity and privacy requirements that must be met in order to transfer [location] information, or authorize the release or representation of such information through

an agent.

In essence, the working group will create a specific format for the expression of location privacy and security preferences. The way those preferences are expressed and enforced will likely have a broad impact on user privacy and control. Although this effort has similarities to the P3P protocol of the World Wide Web Consortium, it will be tailored to some unique characteristics of location information. Critically, the new platform is expected to include default privacy requirements to be applied in the absence of any privacy rules created by a user.

The CDT Standards Project has been actively involved in the GEOPRIV working group since its first meeting in August 2001:

- Last fall, working with Deirdre Mulligan of the Samuelson Law, Technology, and Public Policy Clinic at Berkeley, CDT submitted to the IETF an Internet-Draft entitled "Framework for Location Computation Scenarios." The Internet-Draft offers initial analysis of the location-tracking situations in which privacy must be protected.
- In collaboration with a technologist from Siemens AG in Germany, as well as Deirdre Mulligan, CDT is working on two additional documents: a "requirements" draft specifying what technology must be created, and a "scenarios" draft specifying range of the situations in which the technology must work as designed. On May 8, 2002, we submitted the first of these in an Internet-Draft entitled "GEOPRIV requirements."
- The "GEOPRIV Requirements" draft will be the primary focus of an Interim Working Group Meeting to be held in June. We are hopeful that the draft will be formally endorsed by the working group, and finalized at the Yokohama IETF meeting in July 2002.

Following the July meeting, the Standards Project will continue to provide updates on the progress of the GEOPRIV working group effort. Under its current charter, the work of GEOPRIV is not expected to be completed until early 2003.

For more information:

GEOPRIV Charter: http://www.ietf.org/html.charters/geopriv-charter.html

"Framework for Location Computation Scenarios," Internet-Draft, November 2001:
http://www.cdt.org/standards/draft-morris-geopriv-scenarios-00.txt (original text format),
http://www.cdt.org/standards/draft-morris-geopriv-scenarios-00.pdf (PDF format)

"GEOPRIV Requirements," Internet-Draft, April 2002:
http://www.ietf.org/internet-drafts/draft-cuellar-geopriv-reqs-02.txt (original text format),
http://www.cdt.org/standards/draft-cuellar-geopriv-reqs02.pdf (PDF format)

---

2 - Standards Update: Quick Dispatches on Standards & Policy

a. OPES GRoup Considers Importance of PRESERVING End-to-End Data Integrity. IETF's working group on OPES (Open Pluggable Edge Services) has received guidance from the Internet Architecture Board. OPES deals with services that can reside between a client and a server on the Internet, such as a web proxy cache or other intermediary. CDT submitted comments noting that such services raise serious concerns about the integrity of end-to-end communications, and could enable tampering or censorship. In its considerations document, the IAB recognized the importance of notice and consent

when such systems are used, so that possible negative impacts are minimized. In an upcoming Standards Bulletin, we will provide an in-depth analysis of OPES.

CDT's original comments on OPES are at http://www.imc.org/ietf-openproxy/mail-archive/msg00828.html. The IAB's analysis of OPES is at http://www.ietf.org/rfc/rfc3238.txt. The charter of the OPES working group is at http://www.ietf.org/html.charters/opes-charter.html. The home page of the OPES working group is at http://www.ietf-opes.org/.

- New Cross-Registry Information Service Protocol (CRISP) Proposed As Successor to Whois. At last March's IETF meeting, experts convened in a "Birds of a Feather" (BOF) meeting to brainstorm on a new directory protocol for domain name registries. The current protocol, WHOIS, stores data about domain name registrants, but its uses have broadened substantially over the years to include law enforcement and intellectual property enforcement uses. Controversies about access and privacy have arisen, and a desire has emerged to reevaluate the system. CRISP raises important policy questions that could have a serious impact on users. The protocol is still in the formative stages and has not yet been recognized as an IETF working group, but CDT has been closely monitoring their work so far.

The Agenda and discussion of CRISP BOF can be found at http://www.ietf.org/ietf/02mar/crisp.txt.

- IEPREP Working Group Begins Emergency Preparedness Activity. The IETF's new working group, IEPREP (Internet Emergency Preparedness), is poised to address key questions about Internet use in an emergency situation. Operating on a short timeline, IEPREP will develop guidelines for Internet technologies that will be needed to enable rapid response to a major emergency, but also raising issues of equity and access by the public to important services in times of crisis. The group hopes to finish the bulk of its work by August 2002.

The Charter of the IEPREP working group can be found at http://www.ietf.org/html.charters/ieprep-charter.html.

- Standards and Intellectual Property. Both the IETF and W3C are wrestling with important intellectual property issues. Internet standards developed by both organizations have historically been publicly available on a royalty-free basis, but with increasing regularity, the work of standards groups has slowed because proposed standards implicate technologies covered by software patents. A long-term system to resolve or avoid patent and other IP-related disputes is needed and CDT is following these developments closely. The W3C is actively revising its patent policy, and the leadership of the IETF has indicated that such an effort is on the horizon.

The home page of the W3C Patent Policy Working Group can be found at http://www.w3.org/2001/ppwg/.

- Upcoming IETF-54 Meeting in Yokohama, Japan. The second of the IETF's three 2002 in-person meetings will begin July 14 in Yokohama, Japan. IETF meetings frequently catalyze working group activity and lead to new creativity in the standards process. Although most of the working groups' substantive work is conducted online, the critical progress on challenging issues can often be made at the meetings. John Morris, Director of CDT's Standards Project, will be attending IETF-54; feel free to contact John with any questions or comments about the meeting. CDT will continue to provide updates on the meeting's progress.

The home page of IETF-54 home page can be found at http://www.ietf.org/meetings/IETF-54.html.

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

CDT POLICY POST
Volume 8, Number 14, June 11, 2002

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

CONTENTS:

---

(1) FEDERAL COURT RULES LIBRARY FILTERING MANDATE UNCONSTITUTIONAL In a major victory for free speech online, a federal court in Philadelphia on May 31 rejected as unconstitutional a law that would have required nearly every library in America to install and use Internet filtering software. The three-judge panel unanimously ruled that the Children's Internet Protection Act, passed by Congress in late 2000, was overbroad, and would violate the First Amendment rights of library patrons, both adults and minors. The court therefore ordered that the law not be enforced.

Plaintiffs in the case -- which included the American Library Association, the American Civil Liberties Union, and a wide assortment of libraries and library patrons -- emphasized the serious over- and under-blocking problems in Internet filtering software. They argued that use of such software by libraries would deny patrons access to a large amount of constitutionally protected online material. In its lengthy opinion, the court agreed.

CDT strongly supports the court's decision, and views it as another important signal that heavy-handed content regulation is the wrong approach to protecting children on the Internet.

The decision of the Eastern District of Pennsylvania can be found at
http://www.paed.uscourts.gov/documents/opinions/02D0414P.HTM

---

(2) CONTROVERSIAL LAW ATTEMPTED TO LINK FEDERAL LIBRARY FUNDS, FILTERING The Children's Internet Protection Act (CIPA) was passed by Congress in 2000 as part of a large appropriations package. After two previous attempts at regulating online publishers -- the Communications Decency Act (passed in 1996) and the Children's Online Protection Act (passed in 1998) -- were rejected by the courts as unconstitutional, CIPA attempted to limit access to certain kinds of Internet content by users in public libraries and schools. The district court's ruling blocks enforcement of the provisions of CIPA involving public libraries, but does not address the provisions affecting schools, which still remain in effect.

CIPA attempts to make the federal government's funding of libraries and schools contingent upon their use of Internet filters. A very large percentage of both libraries and schools receive federal support to help defray the ongoing costs of providing Internet access and other services, but CIPA would eliminate that funding for any library or school that does not install and use Internet filtering software on all Internet-enabled computers. CIPA requires that these filters be equipped to block access to child pornography, obscenity, and material "harmful to minors." Adults wishing to access material that is constitutionally protected but "harmful to minors" would be required to request that the filter be disabled.

CDT opposed CIPA's passage and strongly supports the court's decision to enjoin CIPA's enforcement. We recognize that while filters are imperfect tools, when used voluntarily by families with parental supervision, they can help keep offensive material away from children. Federally mandated use of those filters, however, denies American's access to material they are entitled to view under the First Amendment. In addition, when required by government, filtering imposes a "one-size-fits-all" approach to managing online content that denies the diversity of American communities. It forces communities to endure the costs of filters -- namely, their tendency to overblock constitutionally-protected material -- without considering other options that might better serve their interests. The court correctly found CIPA's approach unconstitutional.

---

(3) OPINION EVALUATES FILTERS, RECOGNIZES INTERNET AS A UNIQUE PUBLIC FORUM The Court's opinion discusses in detail the ways popular Internet filtering programs are designed and operate, and identifies their tendencies to both under-block (permit a user to access inappropriate or unwanted material) and over-block (block access to appropriate, desired material). After a nine-day trial in which both sides presented significant expert testimony, the court expressed strong reservations about the effectiveness of Internet filtering technologies, and was unconvinced that their use could be required in public libraries without running afoul of the First Amendment.

The court also rejected the government's argument that CIPA's constitutionality should be examined only at a relatively low level of scrutiny. In particular, the court disagreed with the notion that the use of Internet filters to block access to certain kinds of Internet content was akin to libraries' exercise of discretion in other decisions about the content of its collection. Because of the Internet's unique potential as a medium of expression and communication, the court held that any attempts to regulate Internet content must be subjected to the highest level of scrutiny.

---

(4) GOVERNMENT LIKELY TO APPEAL RULING TO THE SUPREME COURT The district court's rejection of CIPA is unlikely to be the end of discussions over the constitutionality of federal filtering mandates. One provision of CIPA, unaffected by the court's decision, permits the government to appeal the district court's decision directly to the Supreme Court on an expedited basis. Many observers expect the case to be appealed. If it is appealed, and if the Supreme Court agrees to hear the case, arguments would likely be held in late 2002 or early 2003, with a final decision on CIPA's constitutionality possibly coming in Spring

or early Summer of 2003.

---

(5) EDUCATION AND ENFORCEMENT ARE THE BEST PATHS TO ONLINE SAFETY The district court's rejection of CIPA marks the third time that legislation attempting to protect children online by restricting content or access to content has been found unconstitutional by the courts. In the meantime, several studies, including the Report of the Commission on Children's Online Protection Act, and the recently released National Research Council report, "Youth, Pornography and the Internet," have concluded that legislation simply will not work to protect children from inappropriate material online.

This unproductive cycle of legislation and litigation, beginning with passage of the Communications Decency Act in 1996 to the Children's Online Protection Act in 1998 to CIPA today, does little to serve children and families online. CDT believes that giving users control over what they see and do online -- through education and through tools such as those collected at sites like http://www.getnetwise.org -- will more effectively protect kids in ways consistent with their own family values, and with the Constitution.

Instead of passing new laws that do little to address the majority of adult content that is now overseas, the government's appropriate role is to encourage and foster education for children and families about how to assure a safe, positive online experience. It can, in addition, devote increased resources for better enforcement of laws against child predation and child sexual exploitation.

The NRC study, "Youth, Pornography, and the Internet," is online at http://www.nap.edu/books/0309082749/html/. The report of the COPA Commission is available at http://www.copacommission.org/report/.

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

CDT POLICY POST
Volume 8, Number 15, July 24, 2002

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

CONTENTS:

---

(1) HOMELAND SECURITY ACT MOVES THROUGH CONGRESS Congress is moving rapidly to enact legislation to create a new Cabinet-level Department of Homeland Security, with uncertain but potentially large implications for privacy, cyber security and government accountability. The new agency will likely absorb the Coast Guard, the Customs Service, the Secret Service, part of the Immigration and Naturalization Service (INS), and the Federal Emergency Management Agency (FEMA), among nearly two dozen offices and agencies that will be consolidated to improve counter-terrorism efforts.

Here's a brief status report:

- In the House, the bill is H.R. 5005. The latest action occurred on Friday, July 19, when a special select committee marked up and reported the bill, drawing on the recommendations of the various standing committees (Judiciary, Government Reform, Transportation, etc). The Rules Committee is meeting today, Wednesday, July 24, to craft a rule for Floor debate, and the full House is expected to consider the legislation on Thursday and/or Friday, July 25 and 26.

The full legislative history of H.R. 5005 will be available at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR.5005: but Thomas is lagging a little, so you can access the latest version of the bill, the version reported by the select committee, at http://hsc.house.gov/

- In the Senate, the bill is S. 2452, introduced by Senator Joseph Lieberman (D-CT), chairman of the Governmental Affairs Committee, which is marking-up the bill today, Wednesday, July 24.

The Lieberman bill as introduced is posted at http://www.senate.gov/~gov_affairs/072402bill.pdf

---

(2) NEW DEPARTMENT LIKELY TO GAIN AUTHORITY OVER CYBER SECURITY AND INFRASTRUCTURE PROTECTION Both House and Senate bills would grant the Department of Homeland Security authority over cyber security and infrastructure protection. Specifically, the bills would transfer to the new department the functions of the following entities:

- the National Infrastructure Protection Center of the Federal Bureau of Investigation (excluding the Computer Investigations and Operations Section);
- the National Communications System of the Department of Defense;
- the Critical Infrastructure Assurance Office of the Department of Commerce;
- the National Infrastructure Simulation and Analysis Center of the Department of Energy;
- the Federal Computer Incident Response Center of the General Services Administration.

Following objections by the high-tech industry and others, the House bill would not transfer the Computer Security Division of the National Institute of Standards and Technology. The Senate bill as introduced would transfer that NIST component, along with the Energy Security and Assurance Program of the Department of Energy and the Federal Protective Service of the General Services Administration.

Both bills would leave the FBI and CIA untouched by the reshuffling (with the exception of the FBI's NIPC, as noted above).

---

(3) H.R. 5005 CREATES BROAD NEW FOIA EXEMPTION, CRIMINALIZES LEAKS H.R. 5005 contains a controversial provision carving out a new exception to the Freedom of Information Act (FOIA), the 1966 law that promotes government accountability and effectiveness by requiring agencies to disclose information of public interest.

Under the bill that is moving through the House, the Department of Homeland Security could withhold information it receives voluntarily from "non-Federal entities or individuals that relates to" the vulnerability of a critical infrastructure, including the computers that are at the heart of communications, banking, transportation, power and other infrastructures. Much of the U.S. infrastructure is privately owned, and no one has proposed requiring companies to disclose information about their systems to the government. The FOIA exception has been justified as necessary to encourage industry to voluntarily share with the government information about the flaws and vulnerabilities of and attacks on these infrastructures. The language in H.R. 5005 is very broad:

- The FOIA exception in H.R. 5005 is not limited to information which, if disclosed, could be used to harm a critical infrastructure - the language requires withholding of information even if the public interest and the goal of improving homeland security would benefit from its disclosure.
- H.R. 5005 preempts state open government laws, even for information independently obtained by the

states.

- H.R. 5005 provides civil use immunity for information voluntarily submitted to the government, prohibiting the government from using in litigation information submitted to it, even if the information relates to a faulty system that the government owns.

- As we read section 724(h), the bill would also empower the Administration to grant antitrust immunity to selected industries.

- Most remarkably, section 724 of H.R. 5005 includes a provision making it a crime for government officials to disclose information about critical infrastructure vulnerability.

The Senate bill as introduced contained no FOIA language, but at the mark-up today the Governmental Affairs Committee just adopted a FOIA amendment offered by Sen. Robert Bennett (R-UT). The Bennett language, negotiated with FOIA defender Sen Patrick Leahy (D-VT) is much more focused than the House provision and does not include the civil immunity provision, antitrust immunity or any criminal penalties.

---

(4) CONGRESS PROPOSES NEW AGENCY HAVE INTERNAL WATCHDOGS FOR PRIVACY AND CIVIL RIGHTS On the surface of both bills, it appears that the Department will have no new intelligence collection authority, although many of the components being transferred to it (Secret Service, Customs, Coast Guard, INS) have intelligence divisions and will carry their investigative and intelligence authority with them.

Moreover, the new Department will have access to the full range of intelligence information about terrorist threats collected domestically and overseas by the FBI, the CIA and other intelligence and law enforcement agencies. The House bill specifies the Department would have access to all reports, assessments, and analytical information and all information concerning the vulnerability of the US to terrorism, whether or not such information has been analyzed, suggesting that the information obtained by the Department would include raw intelligence. Presumably, the Department also will be able to subscribe to private sector databases. The Senate bill as introduced would give the new Department authority to direct the intelligence agencies to provide (and apparently collect) additional information on specific threats. The Senate bill would also expressly authorize the new Department to engage in data mining and to buy or otherwise obtain private sector databases for that purpose.

Clearly, therefore, the activities of the new Department will raise many privacy issues. As a step towards addressing those issues, the bills include several internal oversight mechanisms.

In the House bill --

- Section 205 requires the Secretary of the new Department to appoint a senior official to assume primary responsibility for privacy policy, including assuring that the use of information technologies sustains, and does not erode, privacy protections and conducting privacy impact assessments of proposed rules of the Department.

- Section 604 requires the Secretary to establish an Office for Civil Rights and Civil Liberties, whose Director shall review and assess information alleging abuses of civil rights, civil liberties and racial and ethnic profiling by the Department.

- Section 204 requires the Secretary to establish procedures on the use of information shared to limit its

redissemination, ensure its security and confidentiality, and provide data integrity. These requirements overlap with the requirements of the Privacy Act, but could provide additional impetus within the Department for careful attention to privacy issues in the handling of personal information.

Similarly, Sections 110 and 111 of the Senate bill would create a Civil Rights Officer and a Privacy Officer.

CDT believes that these provisions need to be fleshed out, either in the legislation or through subsequent Congressional oversight.

- In particular, it should be made clear that guidelines adopted by the new Department on data mining and information privacy should be adopted following public and Congressional consultation and comment.

- Further, Congress should require public reporting of statistical information on sensitive issues, such as descriptions of data mining contracts and arrangements. Such descriptions should include the types of databases "mined" and approximate numbers of persons in each database.

---

(5) HOUSE BILL REJECTS TIPS PROGRAM, NATIONAL ID CARD At the urging of Rep, Richard Armey (R-TX), chairman of the House select committee, the House bill would reject two privacy-threatening initiatives:

- Section 779 of H.R. 5005 prohibits "any and all activities of the Federal Government to implement the proposed Operations TIPS (Terrorism Information and Prevention System)," which would have encouraged delivery men and cable guys to report anything they think may indicate terrorist activity.

- Section 815 states that "nothing in this Act shall be construed to authorize the development of a national identification system or card."

CDT has established a special page where we are indexing materials on the homeland security issue: http://www.cdt.org/security/usapatriot/hearings.shtml

---

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