CDT POLICY POST
Volume 8, Number 16, August 26, 2002

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

CONTENTS:

---

(1) STATE COURT RECORDS GO ONLINE, POSING CONFLICT BETWEEN ACCESS AND PRIVACY

Increasingly, state and county courts are turning to the Internet as a tool to handle caseloads and to open judicial proceedings to the public. More and more courts are using the Internet for case management, online filing of documents, and public access to records.

The trend represents a quantum leap in the openness and thus the accountability of the judicial branch at the local level where most cases arise. However, as state courts put more information online, they are contending with difficult and yet unresolved issues of cost, equity, and especially privacy.

While these issues arise generally in most e-government efforts, they are especially acute in the judiciary's move from paper to electronic systems, given the amount of sensitive financial, medical and other personal information often found in court pleadings.

CDT explored these issues in a report issued last week. "A Quiet Revolution in the Courts: Electronic Access to State Court Records" also provides contact information and links to court records systems online. The report, building on an earlier study done a year ago by the Maryland Advisory Committee on Access to Court Records, documents the rapid pace of change in the online records landscape. Just in the past year, CDT found, court systems in 32 states have reviewed, revised or changed their online records policies .

The full CDT report is available at: http://www.cdt.org/publications/020821courtrecords.shtml

An excellent story by D. Ian Hopper of the Associated Press, with views of state court officials, is available at: http://www.miami.com/mld/miami/news/politics/3909964.htm

---

(2) GUIDANCE TO COURTS IS SLOWLY BECOMING AVAILABLE Neither the federal government nor state governments have any settled policy for putting court records online. However, a variety of national organizations have begun to study how courts can implement electronic access systems while safeguarding privacy.

- One project, carried out with the participation of state court judges and administrators, has drafted a "Model Written Policy for Access to Court Records" and "Guidelines for Policy Development by State Courts." These and related materials can be found at http://www.courtaccess.org/modelpolicy . A final version of the Guidelines is supposed to be released in October.
- The National Consortium for Justice Information and Statistics (SEARCH), in conjunction with the Department of Justice's Bureau of Justice Statistics (BJS), has also examined the issue of privacy and electronic access to court records. In addition to issuing several studies on privacy and court records, SEARCH and BJS sponsored the National Task Force on Privacy, Technology and Criminal Justice Information http://www.ojp.usdoj.gov/bjs/abstract/rntfptcj.htm.
- At the federal level, the Department of Justice's Office of Justice Programs (OJP) has issued three excellent guides on justice information systems: Public Access Guide for Justice Information Systems, Privacy Impact Assessment for Justice Information Systems, and Privacy Design Principles for an Integrated Justice System. (CDT took part in some of the meetings leading to the drafting of these documents.) These guides and related materials are indexed at

  http://it.ojp.gov/sub_topic.jsp?pa=1&SUB_TOPIC_ID=STI-00202&MAIN_TOPIC_ID=MTI-00221&show=yes:
- Beth Givens of the Privacy Rights Clearinghouse outlined some of her recommendations on how to protect privacy in court records in a paper that she prepared for the Computers, Freedom and Privacy Conference this year: http://www.cfp2002.org/proceedings/proceedings/givens.pdf

CDT will continue to monitor these issue and is interested in working with state officials and other interested parties in developing balanced solutions that maximize the values of government accountability, equity and privacy.

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

CDT POLICY POST
Volume 8, Number 17, September 5, 2002

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

CONTENTS:

---

(1) PRIVACY AND SECURITY RISKS IN DRIVER'S LICENSE PROPOSALS The state driver's license has become much more than a license to drive. It is now used as a primary means of authenticating identity in a wide range of commercial and governmental transactions having nothing to do with operating a motor vehicle.

In the wake of the horrific attacks of September 11, some have suggested that we should standardize the design of the state driver's license, add more features to the card and create data systems linked to the card. The new functionality of the card would lead to further reliance on it, including for access control and security screening purposes. Yet, the policy structure for issuance and use of driver's licenses has not kept pace with the increased weight already being placed upon the cards and is totally inadequate for the expansions proposed in the name of fighting terrorism.

One year after the September 11 attacks, there is no evidence that flaws in the design and security of drivers' licenses themselves facilitated the hijackers in carrying out their plans. From what we know, most of the hijackers were not using stolen, counterfeit or altered ID cards. Rather, they were using legitimate state driver's licenses or non-driver ID cards obtained from Department of Motor Vehicle (DMV) offices. The hijackers appear to have obtained these cards using methods that highlight basic problems in the process of issuing ID cards, ranging from weak laws and procedures to the bribery of DMV employees. These problems are not ones that could be cured by introducing more biometrics in the cards themselves or by linking driver's licenses to other state or commercial databases.

CDT Associate Director Ari Schwartz testified today before the House Subcommittee on Highways and Transit on these concerns. Schwartz's full testimony can be found at: http://www.cdt.org/testimony/020805schwartz.shtml

The National Research Council issued a report in April 2002 entitled "IDs -- Not That Easy: Questions About Nationwide Identity Systems": http://www.nap.edu/catalog/10346.html?opi_newsdoc041102

In February, CDT was part of a large coalition urging President Bush not to create a National ID Card: http://www.aclu.org/congress/l021102a.html

---

(2) CDT CALLS FOR MORATORIUM ON NEW FUNCTIONALITY IN DRIVER'S LICENSE Building a linked database of information and adding new functionality to state driver's licenses (chips with financial or biometric information) would add to the demands on use of the driver's licenses and exacerbate the known security problems. Instead, Congress and the states should take four steps:

- Improve the license issuing process -- Fixing the process of issuing driver's licenses is a complex and difficult undertaking, but must be the top priority. In particular, fraud and bribery are rampant in the DMVs and the basic documents used to make decisions about individuals applying for licenses and ID cards are rife with inconsistencies and themselves subject to fraud.
- Improve computer security in the states and federal government -- use and storage of personal information in networked government computer systems continues to grow while computer security continues to lag. Before federal and state governments seek more information identifying individuals, they must prove their ability to protect this information.
- Enact privacy standards for use of the driver's license and baseline legislation for commercial privacy -- The use of the driver's license and other identifiers continues to increase in the commercial sector. Without privacy legislation on the use of personally identifiable information in the commercial arena, Americans will not be protected against the misuse of government identifiers. We need rules addressing when the driver's license or other government ID card can be demanded, what information can be taken from it, how individuals denied access or service can resolve doubts about themselves, how to treat people without cards, etc.
- In the meantime, Congress should declare a moratorium on new features for the driver's license -- Congress should not promote new functionality in a system that we already know is broken. Placing more reliance on the driver's license - such as using it as the centerpiece of an airport security "fast lane" - serves to increase the value of illegally obtained documents at a time when there is a known marketplace for such items.

---

(3) FRAUD RAMPANT AT STATE DMVS While the DMVs have spent time and effort on technologies such as laminates to make counterfeiting more difficult, other forms of fraud have arisen that are of equal or greater consequence. In particular, the fraudulent obtaining of legitimate driver's licenses calls into question the utility of many of the newly suggested biometric features.

The most alarming case of illegally obtained driver's licenses involves the September 11 hijackings. It has been reported that at least 13 of the 19 hijackers obtained valid licenses or non-driver ID cards from Florida, New Jersey or Virginia.

While the Virginia cases have been well documented and involved laws that were immediately changed by the Virginia legislature, many other problems in the issuance process remain across the country. In particular, multiple recent cases involve the bribing of DMV personnel point to a disturbing trend.

- In June 2002, 36 people - including New Jersey DMV employees - were arrested for involvement in a bribery plot in which an unknown number of legitimate driver's licenses were issued illegally.
- In February 2002, 9 people - including 3 New York DMV employees - were charged in a bribery scheme that produced about 100 legitimate driver's licenses.
- Even in the area of commercial licensing - where states have a single database and follow uniform federal standards as required and the under the Commercial Motor Vehicle Safety Act of 1986 (CMVSA) - bribery is common. Such as the well known case in Illinois where at least 175 cases of fraud have been alleged.
- In December 2001, an eight-year employee of the New York DMV was involved in a bribery scheme to steal the personal information of licensed drivers from the DMV computer database over a two-year period indicating that there is already a known market for personal information held by the DMV.

These bribery cases show that the current driver's license and driver's license information are not being adequately protected. Adding new features to the card, such as a smart chip, a biometric identifier and/or a uniform ID number, would increase the value of the card to society and in the marketplace with the result that fraud will increase even as the use of the card increases.

---

(4) JAPANESE PRIVACY PROTESTS OFFER LESSON FOR U.S. Last month, Japanese citizens took to the streets to protest a new government identification system, called Juki Net. In a society that Westerners sometimes assume does not care about privacy, the project touched a nerve.

Juki Net is based on a national database in Tokyo, intended to link a set of personal information--the 11-digit ID number already assigned to all Japanese citizens, plus name, date of birth, sex and address. The goal of the network, in the short term, is to make it easier for individuals to apply for residency cards from anywhere in the country.

But identity theft is a fast-growing crime in Japan. Opponents of Juki Net warned that creating a network that concentrates sensitive information without respect to fair information principles creates a juicy target for identity thieves.

Furthermore, Japan has no comprehensive privacy law for the commercial sector. This means that as essential information, such as the ID number, becomes more centralized and more commonly used, it can be collected, stored, sold and combined with other information with no notice, consent or access and correction rights afforded the individual.

In the face of growing public outcry, several major cities have backed away from involvement. Yokahama, a city of 3.4 million people, has decided to let each resident choose whether to include personal information in the database. The mayor of Kokubnji held an official "disconnecting" ceremony to show the residents of his city that they would not be included in the database at all.

The state of privacy in Japan and the U.S. is strikingly similar. Identity theft has been considered by some officials to be the fastest growing crime in the U.S. Like Japan, the U.S. has no comprehensive law to protect individual privacy in the commercial sector. Marketers have increasingly relied on government-issued identifiers to build and link databases.

For more on Juki Net and its relevance to debates in the U.S., see Ari Schwartz's op-ed in the 8/23/02 Chicago Tribune --

http://www.chicagotribune.com/news/opinion/oped/chi-0208230229aug23.story?coll=chi%2Dnewsopinioncommen
(Registration Required)

English Language Web site of a Japanese national ID system opposition group: http://nationalid.hantai.jp/

---

(5) CONGRESSIONAL PROPOSALS ON DRIVER'S LICENSES In May, Representatives Jim Moran (D-VA) and Tom Davis (R-VA) introduced the "Driver's License Modernization Act of 2002" (H. R. 4633). The bill would require states to turn the driver's license into a "smart card" by including a computer chip on each card. The chip would hold biometric data on the license or cardholder, such as fingerprint information. The chips would be based on private sector standards so that commercial vendors could utilize information and perhaps put their own data on the card. A program would be created to link state motor vehicle databases electronically. Each state would implement procedures for accurately documenting the identity and residence of an individual before issuing a license or card.

This bill mirrors a proposals put forward by the American Association of Motor Vehicle Administrators (AAMVA) and the Progressive Policy Institute (PPI). Senator Richard Durbin (D-IL) is said to be drafting less ambitious, but similar legislation.

The Moran/Davis "Driver's License Modernization Act of 2002" (H. R. 4633):
http://thomas.loc.gov/cgi-bin/bdquery/z?d107:hr4633:

AAMVA's "Special Task Force on Motor Vehicle Security" Executive Summary:
http://www.aamva.org/IDSecurity/idsExecutiveSummary.asp

The PPI's "Using Technology to Detect and Prevent Terrorism":
http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecid=307&contentid=250070

CDT POLICY POST
Volume 8, Number 18, September 10, 2002

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

CONTENTS:

---

(1) FCC ENTERS COPYRIGHT DEBATE, SEEKS PUBLIC COMMENTS As Congress returns from its summer recess, a major debate is unfolding in Washington over future consumer uses of digital programs and content, and digital copyright protection.

The Federal Communications Commission (FCC) has entered the growing debate about copyright policy, asking whether the government should play a stronger role in regulating digital technologies that copyright holders see as threatening control over their intellectual property.

The FCC action came in the form of a Notice of Proposed Rulemaking (NPRM) about something called "the broadcast flag." This is a proposed standard for "marking" commercial digital TV content. VCRs, DVDs and other consumer technologies could be built to "look for" the broadcast flag and limit consumers' ability to make copies of digital-broadcast television programs.

The NPRM, released on August 9, 2002, seeks input from consumers as well as the affected industries on whether a broadcast flag system should be mandated by the government, and if so how. Comments are due by October 30, 2002.

CDT and other public interest groups have urged the FCC to consider the impact such a standard would have on reasonable copying for personal use and the continuing usefulness of consumers' electronic and computer equipment.

The FCC notice is online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.txt

The press release from CDT, Public Knowledge, and Consumers Union responding to the FCC notice is at http://www.cdt.org/press/020807press.shtml

To aid consumers in making their voices heard in this important debate, CDT has created an online resource that you can use to electronically file comments at the FCC. See more about this online comment resource below.

This Policy Post offers some background on this complex but far-reaching issue.

---

(2) HOLLINGS BILL ON DIGITAL RIGHTS MANAGEMENT STALLED Earlier this year, the debate over digital rights management focused on a bill drafted by Senate Commerce Committee chairman Ernest "Fritz" Hollings (D-SC). Sen. Hollings' bill, named the Consumer Broadband and Digital Television Promotion Act (CBDTPA), would have broadly required that digital devices have a built-in "copyright monitor" that prevents the unauthorized or unlawful copying of protected works. The bill would have covered a wide range of consumer technologies -- from personal computers to MP3 players, from CD burners to Personal Digital Assistants to future incarnations of TiVo and ReplayTV.

Some backers of the Hollings bill claimed that its purpose was simply to compel the content community and the technology community to work better together in developing solutions for protecting copyrighted works in the digital world. But the bill generated significant public criticism, in part because of its breadth, and it seems unlikely to pass this year.

For more information about the Hollings bill, see CDT's April 5, 2002 Policy Post: http://www.cdt.org/publications/pp_8.06.shtml .

---

(3) IS THE BROADCAST FLAG A PRECURSOR TO BROADER DRM MANDATES? In comparison to Sen. Hollings' CBDTPA, the broadcast flag is a relatively narrow concept focused on digital television. But it poses the question of whether the government should require that future TVs - and anything that can receive a TV signal, including computers - must be designed to look for the broadcast flag and limit consumer copying accordingly. That, in turn, raises serious questions about the impact on consumers' ability to continue to use their current computers and DVD players and other equipment on copyright-protected material and to copy and manipulate legally-acquired content for personal use, in ways that digital technology empowers them to do.

The debate not only affects consumers, but also puts several important industries at odds. A policy that goes too far in limiting technologies in order to protect copyrighted works may hurt the consumer electronics, information technology, and telecommunications industries, while the producers of content (the film, music, book, and software industries) could be hurt by a policy that ignores the harm that copyright infringers can do armed with computers and facilitated by the global Internet.

The recent flurry of attention surrounding the broadcast flag proposal has been generated by policymakers' eagerness to speed the transition of broadcast television from lower-resolution analog TV (what we view now) to higher-resolution digital TV. Content companies have argued that a broadcast-flag scheme must be put in place before they can safely release high-quality digital content to be broadcast in the clear over the

public airwaves. Their concern is that it will be relatively easy for copyright infringers to capture high-quality digital broadcasts, and infringing copies will flood the Internet and "pirate" marketplaces around the world.

Earlier this summer, the staff of the House Commerce Committee and its chairman Rep. Billy Tauzin (R-LA) asked CDT, Public Knowledge, and Consumers Union to comment on the broadcast-flag proposal from a consumer perspective. In our comments, we made the following points:

- We acknowledged the importance of protecting copyrighted works.
- We questioned whether the broadcast-flag proposal would significantly reduce infringement and whether it would serve its goal of prompting deployment of digital TV.
- We asked about the cost and the impact on legacy equipment (i.e., would material with a broadcast flag play on older equipment?) and reasonable consumer expectations for copying (i.e., will consumers still be able to record their favorite programs and watch them later?)
- We stressed that consumers had been mostly excluded from the policy discussions concerning the broadcast flag and other technology-mandate proposals.

The comments of CDT, PK and CU are online at http://www.cdt.org/copyright/020719bpdg.pdf

---

(4) USER PRIVACY ALSO AN ISSUE IN RIAA V. VERIZON DISPUTE The privacy of ISP subscribers has also become an issue in the copyright debate this September. In a lawsuit in U.S. District Court in Washington, the Recording Industry Association of America has sued a major ISP, Verizon, to reveal the identity of a customer allegedly using a peer-to-peer trading system to share copyrighted songs on his or her computer.

At issue is a provision of the Digital Millenium Copyright Act which requires ISPs to reveal a subscriber's identity based on allegations of infringing material placed on the ISP's systems (such as chat groups or web hosting.) This subpoena power has not been widely used to reveal the identity of subscribers based on material they might have solely on their own computers.

CDT believes that major privacy concerns are raised by allowing any copyright holder (a huge number of people) to compel disclosure of the sensitive identity information of any Internet user, based on a mere allegation that a copyright has been infringed on the users own computer. These disclosures happen without any notice to the user or any meaningful opportunity to challenge the subpoena. CDT commends Verizon for defending the privacy of its users. We look forward to finding a more balanced approach to meeting copyright owners' requests for information.

---

(5) MAKE YOUR VOICE HEARD IN THE COPYRIGHT DEBATE As copyright-related issues move to the forefront here in Washington, consumers need to pay attention. At the heart of these debates is this question: Now that computers and the Internet have made it easy to copy copyrighted works, what kinds of limits should the law put on these technologies in order to protect against the threat they pose for the copyright industries?

The answer to this question will unquestionably have an impact on ordinary citizens. We value the creative works produced by copyright holders, but we also have come to expect to be able to use those works -- especially the copies we pay for -- in increasingly flexible ways (as when we time-shift a favorite TV show

with a personal video recorder or "burn" a collection of songs from albums we own to make a dance mix on CD). These new technologies have already proved to be exceedingly empowering for ordinary individuals who see computers and the Internet not as a means of getting music for free but as new channels for creativity, inquiry, self-expression, and democracy itself.

These are values policymakers must consider and preserve as they develop solutions for new copyright problems in the digital age.

The FCC acknowledged the importance of considering the consumer impact of any technology mandate and raised in its notice many of the same questions that we raised in our response to Chairman Tauzin.

Now you can make your voice heard. For more information on the FCC notice and an online comment submission form, please visit http://www.cdt.org/action/copyright/

CDT POLICY POST
Volume 8, Number 19, September 17, 2002

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

CONTENTS:

---

(1) USE OF THE WEB IN ELECTION CAMPAIGNS NOW THE NORM With the end of the primaries, election 2002 has kicked into high gear. It is clear that candidate Web sites and online voter education guides have become standard tools for candidates and promoters of voter awareness.

CDT takes this opportunity to highlight some of the online resources that are helping improve electoral democracy. These include:

- Non-partisan online voters' resources providing information about all candidates in selected races.
- Guides for candidates seeking to use the Web - do's and don't's of online campaigning.
- Tips for creating online voter education guides for both advocacy-oriented and non-partisan groups.

To keep up to date on election and campaign resources, we recommend joining Steve Clift's Democracies Online Newswire -- http://www.e-democracy.org/do/

Steve maintains a comprehensive list of 2002 U.S. Election News, Information and Links at http://www.e-democracy.org/us/

---

(2) NON-PARTISAN ONLINE VOTERS' RESOURCES OFFER INFORMATION ON CANDIDATES Several

years ago, there was a rush by for-profits companies to create political Web sites. Most of those efforts folded with the bursting of the dot-com bubble, but the quality of the remaining resources has improved. Most of these are now run by nonprofit groups, government agencies or a collaboration between the two. Here are a couple of the best:

- DemocracyNet (DNet) -- http://www.dnet.org

DNet is an interactive Web site designed to improve the quality and quantity of voter information and create a more educated and involved electorate. Founded by the Center for Governmental Studies, DNet is now a project of the League of Women Voters Education Fund. The site encourages candidates to address a wider range of issues, and in greater depth, than they might in other media. On DNet, candidates debate their positions in an "electronic town hall" before on-line audiences. Voters can email candidates directly to ask questions, to volunteer or to make donation. Voters can also submit questions to be posed to all the candidates in a race.

DNet is easy to use. Candidates can enter their positions directly, without any editing. And voters enjoy one-stop shopping for information on candidates, ballot measures, campaign finance information, political parties and elected officials, all based on zip code.

- Michigan's Publius Voter Information Center -- http://www.michigan.gov/sos or http://sos.publius.org

In the 2000 election, it became evident that many citizens could not confirm whether they were registered to vote or to see what a ballot looked like before they got to the polling booth. Many state governments and public interest groups have tried to solve this problem using online systems. Yet most either do not provide enough information or put privacy at risk in trying to confirm the identity of users. From what CDT has seen, Michigan is the first state to get it right.

Working with the Secretary of State, a Detroit based group called Publius has developed the Voter Information Center. The site asks a voter's name, but limits the collection of personal information to only the amount needed to confirm a registration. Once registration is confirmed, the voter is given polling place information (including a map); a mock-up ballot with links to candidate Web sites; instructions on how to use the voting equipment at the polling place; and a voting calendar. Thus, tailored information is provided to users without sacrificing privacy. This Michigan system should serve as a national model.

Non-profits in Minnesota http://www.myballot.net and California http://www.smartvoter.org have also put together excellent systems to provide almost the same level of information available in Michigan.

---

(3) HOW CANDIDATES CAN MAKE BETTER USE OF THE WEB While almost every candidate today has a Web site, very few use them effectively. A new tool put out by the Institute for Politics, Democracy & the Internet provides the best how-to guide we've seen so far: "Online Campaigning 2002: A Primer" -- http://www.ipdi.org/primer2002.html

Drawing on conferences, surveys, interviews, field research,news reports and academic studies, the Institute has amassed an amazing amount of information into a concise (and free!) resource.

CDT especially highly recommends that all campaigns take a look at the Primer's "Best Practices Checklist." Aside from the fact that the list will be used by the Institute and others to review campaign sites for praise and scorn, it also offers the best guide available on how to make sites interactive and accessible to voters, volunteers and community groups.

---

(4) TIPS FOR ORGANIZATIONS CREATING ONLINE VOTER EDUCATION GUIDES For years libraries, the news media and nonprofit organizations have made printed voter's guides to help educate the public on candidate's positions on issues. Effective use of the Web can make these guides available to more people at a lower cost. However, many groups have simply put the printed version of their guides online or have otherwise failed to make use of the Internet's potential for presenting information in new ways.

One of the leading groups providing educational materials for voters, the California Voter Foundation (CVF), has now put together a resource to help promote best practices in the creation of online voter guides. "How to Make an Online Voter Guide: Quick Tips for the Voter Educator" -- http://www.calvoter.org/manual/quicktips.html offers a quick and easy-to-follow set of tips in creating these important resources.

CVF's own Online Voter's Guide http://www.calvoter.org/2002 serves as a model. The site gives voter's a comprehensive overview not only of the candidates and their donors, but also detailed information on the often confusing ballot propositions that continue to mark California's elections.

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

CDT POLICY POST
Volume 8, Number 20, September 20, 2002

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

CONTENTS:

---

(1) CDT & OTHER ADVOCATES OPPOSE DOJ REACH FOR BROADER SURVEILLANCE POWER In a groundbreaking court case, CDT, the American Civil Liberties Union and other leading civil liberties groups have urged a special panel of federal appeals judges to reject a Department of Justice (DOJ) claim for broader surveillance authority in the name of fighting terrorism. The groups filed a "friend of the court" brief in a case in which the government is seeking judicial permission to conduct criminal investigations of terrorism suspects under the weaker rules reserved for foreign intelligence gathering. Under the DOJ theory, prosecutors could thus avoid stricter rules that the Constitution's Fourth Amendment applies to law enforcement investigations.

The case arises out of a May 17 ruling in which a special federal court held that criminal prosecutors could not invoke the 1978 Foreign Intelligence Surveillance Act (FISA) to initiate, direct or control wiretaps, e-mail intercepts or physical searches. The DOJ appealed, arguing that the Patriot Act adopted in the wake of the September 11, 2001 terror attacks permitted use of the lower standards.

The public interest brief calls the DOJ theory an end-run around the Constitution. CDT and its allies point out that the two word amendment relied on by the Justice Department - stating that "a significant" purpose of FISA surveillance had to be foreign intelligence gathering, instead of the earlier requirement that it be "the" purpose - did not alter the structure of the federal surveillance laws, which govern criminal investigations in national security cases under the stricter rules applicable to all criminal matters. Applying FISA's weaker standards and broader surveillance rules to criminal prosecutions would be unconstitutional, the brief argues.

The case involves a number of firsts. It is the first time that the secret Foreign Intelligence Surveillance Court has issued publicly an opinion endorsed by all the court's judges (and only the second time ever that any opinion of the court has become public). It involves the first time that the government has ever appealed a ruling of the court and therefore the first time that the Foreign Intelligence Court of Review has convened. It is also the first time that public interest groups have had the chance to weigh in on a government surveillance request.

The appeals court held a secret hearing on the government appeal on September 9, following which it asked the DOJ to submit a second brief, which is due September 24.

The civil liberties brief, filed on September 20 by CDT, the ACLU, the Center for National Security Studies, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the Open Society Institute is available in PDF at http://www.cdt.org/security/usapatriot/020919fiscrbrief.pdf

Further background:

The FISA Court's May 2002 Memorandum Opinion and Order:
http://www.fas.org/irp/agency/doj/fisa/fisc051702.html

The Justice Department's August 21 appeal brief ("redacted"):
http://www.fas.org/irp/agency/doj/fisa/082102appeal.html

On September 10, 2002, the Senate Judiciary Committee held a remarkable hearing entitled "The USA PATRIOT Act in Practice: Shedding Light on the FISA Process." Statements of Senators and witnesses are online at http://judiciary.senate.gov/hearing.cfm?id=398

---

(2) CONGRESS CONSIDERS FURTHER WEAKENING SURVEILLANCE STANDARDS The breadth of the Justice Department's argument in the "purpose" case seems may not have deterred Congress from considering further changes to FISA. Earlier this summer, several bills were introduced that would have further weakened the Act's standards.

S. 2659, sponsored by Sen. Michael DeWine, would lower the standard for obtaining FISA orders for electronic surveillance orders and physical searches from "probable cause" to "reasonable suspicion," where the target was not a US citizen or permanent resident alien. S. 2586, sponsored by Senators Charles Schumer and Jon Kyl, would define certain individuals as "foreign powers" under FISA.

On Wednesday, July 31, CDT Executive Director Jerry Berman testified before the Senate Select Committee on Intelligence, strongly opposing both bills. Among the main points from CDT's testimony:

- A primary lesson from September 11 is that the government is incapable of analyzing the vast amount of information it already collects. Lowering FISA's requirements would only make that problem worse.
- S. 2586 stands FISA on its head by designating individuals themselves as foreign powers, allowing the secretive and powerful FISA procedures reserved for our nation's fights against foreign groups to be turned against individuals acting alone.
- S. 2659 would allow FISA warrants to issue without probable cause, but the Constitution expressly requires a probable cause finding for all searches.

CDT's testimony is available at http://www.cdt.org/testimony/020731berman.shtml

Other testimony is at http://intelligence.senate.gov/0207hrg/020731/witness.htm

---

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

CDT POLICY POST
Volume 8, Number 21, October 3, 2002

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

CONTENTS:

---

(1) SOME POSITIVES IN NEW ICANN AGREEMENT, BUT KEY FEATURES ARE MISSING On September 20, the U.S. Department of Commerce renewed its Memorandum of Understanding (MOU) with ICANN (the Internet Corporation for Assigned Names and Numbers), the controversial organization that oversees the Internet's core numbering and addressing functions. The MOU authorizes ICANN to continue its activities for another year while laying out a "checklist" of reforms and activities for the next year.

Although there are several positive developments in the MOU, it misses the mark on others and is generally a missed opportunity. Most positively, the new agreement extends ICANN's mandate for just one year and requires regular status reports -- a signal that there may be increased and much-needed oversight of ICANN by the U.S. government this year. The MOU also presses ICANN to make progress on issues of accountability, transparency, and the security of the systems it administers.

Tough talk from Commerce about the MOU was not matched with tough action, despite the government's "frank disappointment" with ICANN's slow progress. The new MOU does not impose any real constraints on the scope of ICANN's powers and authority, leaving the door open to unaccountable and potentially harmful regulation of the Internet by ICANN. It also permits ICANN to continue skirting the issue of giving the Internet public a meaningful voice in its governance.

While a step forward, the MOUÕs renewal is a missed opportunity to effect substantive reform at ICANN, deferring yet again the changes needed to stabilize ICANN and make it accountable for its actions.

The new MOU is available at
http://www.ntia.doc.gov/ntiahome/domainname/agreements/amend5_09192002.htm

The Department of Commerce's public statement is available at
http://www.ntia.doc.gov/ntiahome/domainname/agreements/docstatement_09192002.htm

---

(2) MOUÕs SHORT TERM, TIGHTER OVERSIGHT PUT ICANN UNDER SCRUTINY ICANN's authority over critical Internet functions means that accountability, transparency, and representation are of the highest importance for it. ICANN's power ultimately derives from its MOU with Commerce; if ICANN is not conducting itself appropriately, the MOU is a powerful lever for change.

Unlike previous versions, the new MOU places several new requirements on ICANN and tightens Commerce's oversight, incorporating several items recommended by CDT and other observers.

The MOU obliges ICANN to improve the transparency of its policymaking and requires it to advance long-delayed accountability provisions that would establish outside review of contentious decisions. Commerce stated that it expects "significant advancement" in these and other areas within a year.

The MOU also requires quarterly reports, publicly posted, which will clarify ICANN's priorities and press it to show results.

Commerce also assumed several new responsibilities for itself, including outreach to other governments to clarify their relationship with ICANN.

As a group, these provisions set the stage for closer monitoring of ICANN by the Department of Commerce, pressuring ICANN to make needed reforms expeditiously. CDT welcomes this additional oversight and will be watching its implementation closely.

CDT's Letter to the Department of Commerce is available at
http://www.cdt.org/dns/icann/020819comments.shtml

---

(3) ICANN MUST ADDRESS MISSION LIMITS, REPRESENTATION ICANN remains a highly controversial organization, but the new MOU does not include some key reforms ICANN must undertake if it is to ever achieve legitimacy in the eyes of Internet operators. In particular, it is critically important that ICANN clarify its mission and establish limits to its authority, and that a mechanism for representation of user and public interest voices be established.

ICANN's management of key Internet systems gives it potentially far-reaching authority to set global policies, even in areas it was not designed for, like content control. Until there are clear limits on ICANN's ability to engage in appropriate economic or social regulation, key elements of the Internet community will not trust ICANN as a credible authority, corroding ICANN's effectiveness and long-term survival. The MOU does not explicitly press ICANN to adopt such limits to its powers, making it a missed opportunity.

The new MOU also misses a chance to put ICANN back on track regarding the representation of the user voice. While CDT acknowledges that direct elections are not favored by many, ICANN has effectively abandoned all plans to provide users and public interest groups with a real role in selecting members of the ICANN Board of Directors. By remaining silent, the MOU can be read as tacit approval of ICANN's rejection of user representation, casting serious doubt on ICANN's long-term prospects for global legitimacy.

CDT still believes in private sector management of key Internet coordination functions. Adoption of clear, effective mission limits, and establishment of representation for the user voice, must be undertaken seriously if ICANN is to become a legitimate, trusted manager for Internet users worldwide.

---

(4) UPCOMING ICANN MEETING IN SHANGHAI, OCTOBER 27 - NOVEMBER 1 ICANN's agenda for the next year, including the fulfillment of its MOU obligations, will be largely set at its upcoming quarterly meeting in Shanghai, China, at the end of October. The agenda is expected to include the Board's final approval of its "Blueprint for Reform." CDT and others have noted serious flaws in the Blueprint, including the lack of mission clarity and representation noted above. CDT Associate Director Alan Davidson will attend the Shanghai meeting to monitor and comment on ICANN's activities.

ICANN may also take some transitional action with regard to the nine Board members whose terms are set to expire at the Shanghai meeting. Five of the Directors scheduled to leave the Board are the "At-Large" Directors elected in 2000; unless changes are made, their departure will mark the end of direct user representation at ICANN. Moreover, if no new Directors are selected, ICANN will be left with a Board of just nine Directors to oversee large-scale organizational reform, raising serious accountability questions.

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

CDT POLICY POST
Volume 8, Number 22, October 25, 2002

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

CONTENTS:

---

(1) WHAT DOES THE SNIPER CASE REVEAL ABOUT POLICING, TERRORISM AND DATABASES?
Already the argument has been made on at least one list that "Big Brother caught the sniper" - that the person who was terrorizing the Washington, DC area was caught police by using massive government databases, citizen informants, and inter-agency government information sharing.

We see it differently: The suspected sniper was caught in part using government databases consisting of carefully-defined information collected pursuant to strict guidelines and subject to privacy protections; a citizen responding to leaked (arguably illegally leaked) government information of a precise nature; and traditional police work (including one officer's telephone call to another police officer he knew personally and the non-electronic exchange of information). Most importantly, though, it seems that the case was broken when the alleged sniper (or someone who knew him) called police and gave them crucial information.

While there are several pieces of the investigation that we don't know full details about yet (e.g., how did police trace the call to the priest near Ashland, VA), nevertheless it is useful to look at some the databases and methods the police used, for they offer lessons for current privacy and security debates.

---

(2) FINGERPRINT DATABASES USEFUL DESPITE - IN PART BECAUSE OF - PRIVACY RULES The alleged sniper was identified in part because a fingerprint lifted from a Montgomery, Alabama robbery-murder was matched with a fingerprint taken by law enforcement authorities from the 17 year old companion of the

accused following the youth's arrest in connection with an altercation in Washington state.

Background on fingerprint databases: What became the International Association of Chiefs of Police (IACP) was founded in 1893 when police chiefs from all parts of the country met in Chicago to form an organization to share information across jurisdictions and apprehend wanted persons who fled local jurisdictions. In 1897, they created the National Bureau of Criminal Identification, just as the technique of fingerprinting was becoming popularized. In 1924, the IACP's criminal identification files (fingerprints and rap sheets) were turned over to the federal government and used to create the FBI Identification Division, sixty years before 1984's Big Brother.

But the key point is this: The database at issue (actually now a networked series of databases) is woven through with a series of rules intended to limit its use and protect privacy.

- First of all, the fingerprint database at issue consists only of people who have been arrested. That is, they are people for whom there was probable cause to believe that they had already committed a crime. (Small exceptions: unidentified dead and certain missing persons.)
- Second, all information in the database is collected with the knowledge of the record subject.
- Third, access to the federal database is strictly controlled by statute and regulation - by and large, it is available only to law enforcement agencies, and to government agencies and some private sector employers conducting background checks, but only when the legislature has specifically determined that the occupation requires a criminal history check.
- Huge efforts have been made over the years to improve the data quality of the database, particularly in making sure that it is complete. In recognition of the data quality problem, particularly the fact that the disposition of many arrests are not posted, the federal courts have ruled that it is a violation of federal law to use mere arrests in the database as the basis for employment decisions.
- When the database is used for non-criminal justice purposes, it is accessed only with prior written consent of the record subject - a very high standard.
- Individuals have a right to access any and all information about themselves that is in the fingerprint/rap sheet database and they have the right to obtain the correction of erroneous or incomplete information. There are also laws providing in some cases for sealing or purging of information.

Notwithstanding all of these protections - in some respects, particularly the data quality initiative, because of these protections - the database is very useful to law enforcement agencies.

---

(3) CAR LICENSE PLATE DATA ALSO SUBJECT TO PRIVACY PROTECTIONS The use of car registration databases also is a very interesting example of the rules and privacy protections that have been built up around government databases: The Department of Motor Vehicle (DMV) databases are very useful to law enforcement despite being subject to a number of privacy protections.

- First, the identifying data are collected only with notice and express prior consent - meaning that everyone in the DMV database knows he is there, was expressly asked to be put in the database, and has a right of access to all information about himself in the database. (In fact, practically everyone in the DMV database carries with himself or herself a copy of the information in the database.)
- The information is quite highly accurate. It is regularly updated. Individuals can easily change inaccurate or outdated information. They can purge erroneous information (for example, when they move or get married or divorced and change their name).
- The database contains a numerical identifier, but several states, recognizing the privacy and security flaws in the use of the Social Security Number as a single identifier, have allowed their citizens to

choose a random number for use in the DMV system, with no degradation in its value for administration of the drivers license system or its value as an identifier for other criminal law enforcement purposes.

License plate data is especially interesting in terms of some of the authentication debates taking place in other contexts, for while each license plate contains a unique number, it is not a personal identifier: the person driving the car need not be the person in whose name the car is registered.

Also both drivers license data and car registration data are subject to privacy protections. In fact, Congress has adopted a very detailed law (upheld against constitutional challenge by the US Supreme Court) limiting the use of DMV data.

---

(4) CITIZEN TIPSTERS - A RIGHT WAY AND A WRONG WAY Contrast the tip that led to the alleged sniper's arrest to the TIPS program suggested by the Bush Administration earlier this year. In the sniper investigation, the police put out a general request for information about suspicious people, posting a hot line number, similar to the hot line number the Justice Department was proposing for the anti-terrorism TIPS program. In the sniper case, the TIPS line generated over 70,000 leads, which consumed huge resources but apparently contributed nothing to the solving of the case - except for the calls that the sniper himself made to line, some of which police ignored or discounted apparently overwhelmed by the number of crank calls.

In contrast, the "tip" that led to arrest of the suspects related to a very specific piece of information - a license plate number.

Ironically, the government had not officially made the license plate number public. It was leaked by one or more officers violating (at the very least) the conditions of their employment and the orders of their superiors. This is very interesting in this era of talk about "information sharing," which too often means sharing with a few while keeping from the public. Legislation is now pending in Congress that would make it a crime for a government official to disclose to the public information about cyber-vulnerabilities that has been given the government by the private sector. If a similar criminal penalty had been in place for law enforcement investigative information, the officers who leaked the license plate might have not taken the risk and the sniper might still be on the loose.

See "The Leak That Sank the Suspects" by Howard Kurtz in the October 25 Washington Post: http://www.washingtonpost.com/wp-dyn/articles/A13610-2002Oct24.html

---

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

CDT POLICY POST
Volume 8, Number 23, November 4, 2002

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

CONTENTS:

---

(1) US ELECTION DAY - NOVEMBER 5 - MAKE DEMOCRACY WORK: VOTE!Next Tuesday, November 5, is Election Day. CDT is strictly non-partisan, but we can tell you this: VOTE!

The Internet is not immune from law and regulation. What elected officials do in Washington, in the states, and even at the local level will affect the future of the Internet - whether it remains open, decentralized and user controlled, a medium for innovation and free expression.

We urge you to exercise your democratic right and fulfill your civic duty by voting on Tuesday, November 5. Many elections this year are likely to be very close. Every vote does matter.

---

(2) 108TH CONGRESS, STATE LEGISLATURES TO CONFRONT HOST OF INTERNET ISSUES On Tuesday, you will be asked to choose the Congress and many of the state legislatures and governors. Next year, they will be confronting a host of issues that will directly affect your use of the Internet and other digital communications technologies.

Key issues that will be on the policy and lawmaking agenda next year include:

- **Copyright** - A major debate is underway over how to protect copyrighted material in the digital age. This year, legislation was introduced in Congress that would have controlled the design of televisions, computers and other electronic devices. Next year, the debate will resume.
- **Privacy** - The privacy concerns of consumers remain unsatisfied. Legislation will be considered in the States and at the federal level.
- **Security** - Oversight of the effectiveness of PATRIOT Act authorities, the prospect of PATRIOT II, and

the creation of a new Department of Homeland Security and its role in computer security are all issues that directly affect Internet users.

- **Free Expression** - Some government officials still want to control what you choose to view on the Internet. Laws continue to be brought up not only at the federal level, but also in the state legislatures, as in the case of a recent Pennsylvania law that authorizes a court to order ISPs to block content with no adversarial hearing and no notice to the content creator.

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

CDT POLICY POST
Volume 8, Number 24, November 7, 2002

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

CONTENTS:

---

(1) DOMAIN NAMES BODY APPROVES RESTRUCTURING PACKAGE IN SHANGHAI At its late-October meeting in Shanghai, China, the Internet Corporation for Assigned Names and Numbers (ICANN) approved sweeping new bylaws in an attempt to refocus and restructure the organization. Among other things, the new bylaws lay out ICANN's intended mission, revamp its process for selecting Directors, and reshape ICANN's policy-making process.

ICANN is responsible for oversight of key central resources for the Internet, such as the domain names system. Since its creation in 1998, ICANN has been a controversial organization, largely due to concerns that it has not been adequately accountable to Internet users and that it has lacked strong limits on its powers. The new bylaws seek to address these concerns about ICANN.

Significant questions still exist about ICANN. Though the new bylaws make progress in some areas, there is continuing need for improvement in others. In particular, ICANN continues to require stronger accountability measures, means for their enforcement, and a narrow, limited mission statement. CDT believes that ICANN needs to evolve significantly over the next several months if it is to prove itself as a credible manager for critically-important online resources.

ICANN's newly-approved bylaws are available at: http://www.icann.org/minutes/minutes-appa-31oct02.htm

---

(2) FURTHER REFINEMENT OF ICANN'S MISSION AND POWERS NECESSARY Further attention to ICANN's mission and the extent of its authority is necessary. Because ICANN exerts authority over critical central Internet functions, its activities must be carefully constrained to avoid abuses of power. If its power is not adequately limited, ICANN in the future could leverage its authority to exert powers never contemplated in its creation and structuring, like content regulation. Effective limits on ICANN can prevent that kind of "mission creep" and, in doing so, increase ICANN's credibility in the Internet community.

ICANN's new bylaws make some progress on this front. They include a statement of its "Mission and Core Values" in which a relatively non-specific set of coordination activities is coupled with a list of values for ICANN to take into account when conducting those activities. However, ICANN remains free to interpret those values broadly, and the mechanisms to enforce any limits on its power are not strong.

CDT believes that the ICANN mission needs further attention. In particular, ICANN needs to commit to acting only when necessary to carry out a narrowly-defined, basically technical mission -- and that it will not act in other cases. Also, ICANN needs mechanisms that will enforce the bylaws' mission limits on ICANN's Board of Directors and other policy bodies.

By developing a statement of mission that is strong and enforceable, ICANN will create an increased level of trust among Internet users and operators, as well as enhancing the efficiency of its own activities. Without such a statement, however, ICANN will continue to lack the confidence of the community it is meant to serve.

CDT has posted a discussion paper on ICANN's mission and activities, with suggestions on establishing a workable definition for both. Available at: http://www.cdt.org/dns/icann/021030cdt.shtml

---

(3) SIGNIFICANT DETAILS STILL NEED RESOLUTION The Board's approval of new bylaws in Shanghai is not the end of the effort to reform ICANN. As ICANN itself noted, major pieces of the ICANN structure still need attention.

At its mid-December meeting in Amsterdam, ICANN is expected to make progress on some of these questions. ICANN's major agenda in Amsterdam will include (1) adoption of as-yet-unwritten bylaws describing how the operators of country-code Top-Level Domains (ccTLDs) -- domains associated with countries, such as .de or .us -- participate at ICANN; (2) revision of bylaws describing ICANN's relationship with the Regional Internet Registries (the bodies that manage the IP address space), and; (3) adoption of a plan to transition from ICANN's current mode of operation to its new structure.

Over the next year, however, other critical questions also require attention. As discussed above, ICANN must continue refining the statement of its mission and activities. It also must demonstrate that public interest voices will be adequately included in its new structure. The new bylaws provide the outlines of an "At-Large Advisory Committee" to fulfill this need, but the ALAC does not yet exist, nor will creating it be an easy task. ICANN should make ensuring the ALAC's success a high priority, and should prepare itself to offer support to the challenging task of building a structure to bring public voices into ICANN's discussions.

---

(4) GOVERNMENTS EYE EXPANDED ROLE AT ICANN At the Shanghai meeting and in recent weeks, there has been heightened discussion about the role governments may seek to play at ICANN. ICANN is a private, non-profit organization; historically, governments have played an advisory role in its activities, but have had no direct influence over ICANN's activities (Note: ICANN's authority ultimately derives from

agreements with the US Department of Commerce; Commerce, however, has maintained a largely hands-off attitude towards ICANN's day-to-day activities). Whether governments should assume an increased position at ICANN has lately become an active issue that could implicate ICANN's future as manager of key Internet functions.

In particular, the International Telecommunications Union (ITU) has expressed interest in having an increased role in domain name policy issues, notably in the form of four resolutions passed at ITU's recent meeting in Marrakesh. The ITU is an international treaty organization, made up of national government delegates, that coordinates the international telephone network. CDT and others, however, remain concerned that expanded involvement by the ITU or other government entities could undercut important goals that informed ICANN's design.

One of ICANN's primary design principles was that it would manage key Internet functions in a private fashion. Private management has generally been viewed as quicker, more efficient, and more adaptive than "top-down" government regulation, as well as potentially more responsive to the quickly-evolving needs of the Internet community. Though ICANN has had difficulty establishing its credibility in several areas, particularly its accountability to Internet users, CDT continues to believe that a non-governmental administrative body can be an effective manager of these key functions. Increased involvement by government agencies threatens could undercut ICANN's chances at such effectiveness.

Moreover, unless ICANN can establish clear limits to its mission and powers, more government involvement could create pressure for ICANN to expand its activities in inappropriate ways. ICANN's authority over key Internet features is not meant to enable the enforcement of national laws at the global level. Though national governments have the authority to exercise sovereignty over their citizens, ICANN should not be viewed as a tool to expand that authority even more broadly.

The ITU's resolution regarding ICANN is available at http://www.itu.int/osg/spu/resolutions/2002/res102.html

---

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

CDT POLICY POST
Volume 8, Number 25, November 21, 2002

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

CONTENTS:

---

(1) NEW LAW TO REQUIRE PRIVACY IMPACT ASSESSMENTS FOR U.S. AGENCIES The E-Government Act of 2002, passed by Congress this week and soon to be signed into law, includes an innovative and potentially far-reaching provision requiring federal government agencies to conduct privacy impact assessments before developing or procuring information technology or initiating any new collections of personally-identifiable information.

Under the legislation, originally introduced by Senators Joe Lieberman (D-CT) and Conrad Burns (R-MT), a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice would be provided to individuals and how the information will be secured. To the extent practicable, privacy impact assessments must be published. The Director of the White House's Office of Management and Budget (OMB) will issue guidelines for the assessments.

CDT believes that the law could have a significant positive impact in three ways:

- The assessments will raise the level of attention to privacy issues within federal agencies, at the most critical stage: before new technology is purchased or new collections of data are initiated.
- The assessments will bring greater transparency to the IT development and procurement process, allowing Congress, citizens and advocacy groups to better scrutinize the privacy decisions of the government.
- Using the massive purchasing power of the U.S. government , the assessments could help to increase the marketplace for technologies that incorporate privacy "by design."

CDT supported the privacy impact assessment provision.

Related legislation, the Federal Agency Protection of Privacy Act (HR 4561), introduced by Representative Bob Barr (R-GA), would have required privacy impact assessments for new agency rules and regulations. That bill passed the House earlier this year but was never taken up by the Senate. Rep. Barr, a leader on many privacy issues, will not be in Congress next year. But his proposal remains valid and a sound complement to the E-Gov Act. We believe OMB should require such assessments as best practices despite not being required in law.

Links to the text and legislative history of the E-Government Act:
http://thomas.loc.gov/cgi-bin/bdquery/z?d107:hr2458: http://www.cdt.org/legislation/107th/e-gov/

A link to the Barr bill can be found at http://www.cdt.org/legislation/107th/privacy/

---

(2) PRIVACY NOTICES, INCLUDING P3P STATEMENTS, NOW REQUIRED FOR AGENCIES The E-Government Act also requires agencies to post privacy notices on their Web sites, detailing agency practices and individual rights. Most agencies already post written privacy notices after the Clinton administration, under the leadership of Chief Privacy Counselor Peter Swire, required them in an administrative order. The new law will take the agencies one step further by requiring "machine-readable" notices, such as those specified in the Platform for Privacy Preferences (P3P) standards.

Under the P3P framework, 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.

Currently, only a few federal agency Web sites are P3P compliant, including the Federal Trade Commission, the US Postal Service and portions of the Department of Commerce.

While privacy notices do not in and of themselves guarantee privacy protection, they offer a basis for public and Congressional scrutiny of agency practices.

For more information about P3P and privacy notices on government Web sites:

- Policy Post 8.09, Privacy Standard Moves Forward, April 26, 2002 -- http://www.cdt.org/publications/pp_8.09.shtml
- P3P Toolbox - http://www.p3ptoolbox.org
- OMB Memorandum M-99-18, Privacy Policies on Government Web sites -- http://www.whitehouse.gov/omb/memoranda/m99-18.html
- Letter from CDT urging posting of privacy policies on federal Web sites, April 15, 1999 -- http://www.cdt.org/privacy/lettertoswire.html

---

(3) E-GOVERNMENT ACT INCLUDES OTHER IMPORTANT PROVISIONS The E-Government Act includes a host of other provisions that could have an impact on how the public interacts with the government. Many of these could have merited free-standing legislation. Most of them have received little attention. At the risk of an overly-long Policy Post, we list some of them here - see the text of the bill for full

details:

- Creates a specific position in OMB for the Administrator of the Office of Electronic Government. Some Members of Congress had wanted to create a Chief Information Officer for the federal government, but the Administration balked. The compromise basically codifies current practice, under which Associate Director Mark Forman heads up e-government efforts. The new position does not have a lot of direct power, but as a statutorily-authorized position it will be subject to more consistent Congressional oversight. Sec. 101.
- Authorizes an E-Government Fund with $45 million in fiscal 2003, an amount that would increase to $150 million by fiscal 2006, to fund the development and implementation of innovative uses of the Internet and other electronic methods by federal agencies. Sec. 101.
- Requires the General Services Administration to establish a framework to allow interoperability among federal agencies when using electronic signatures, including the development of a "Federal bridge certification authority for digital signature capability." Sec. 203.
- Requires each federal court to establish a Web sites where the public could get court rules, decisions, docket information and documents filed with the court in electronic information. The section requires the Supreme Court to adopt rules to protect privacy and security concerns relating to the electronic filing and availability of documents. Sec. 205.
- Requires federal regulatory agencies, "to the extent practicable," to ensure that a publicly accessible federal government Web site includes all information that the agency is required to publish in the Federal Register, and to accept electronic submissions in rulemaking proceedings. Sec. 206.
- Creates a committee to study the adoption of standards to enable government information to be searched across agencies. Sec. 207. A separate section requires a 3 year study of interoperability and the integrated collection and management of data. Sec. 212. Such initiatives have positive implications for electronic Freedom of Information Act requests, but may have negative implications for privacy, allowing even greater amalgamation of personally-identifiable information in the hands of disparate government agencies. A third provision requires OMB and the Interior Department to develop common protocols for the acquisition and application of geographic information (GIS), in order to maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible, something that will be of importance on environmental issues. Sec. 216.
- Requires OMB to develop and maintain a repository that fully integrates information about research and development funded by the federal government. Sec. 207(g).
- Authorizes an IT exchange program under which mid-level information technology managers of the federal government can be detailed to work in the private sector for up to 2 years and private sector employees can be assigned to work in federal agencies. Sec. 209.
- Requires the Administrator of E-Gov to develop an online tutorial explaining how to access government information services and information on the Internet. Sec. 213 (f).
- Requires a National Academy of Sciences study on the digital divide. Sec. 215.
- At the behest of Chairman Tom Davis (R-VA), includes the "Federal Information Security Management Act" (FISMA). The provisions impose certain responsibilities on agency heads, give OMB certain oversight of agency information security practices, mandate annual independent audits of agency computer security practices, and require reports to Congress. The Act also renames the Computer System Security and Privacy Advisory Board (CSSPAB) as the Information Security and Privacy Advisory Board, keeping its dual focus on security and privacy.
- Establishes a very strict rule of confidentiality for information collected by the federal government for statistical purposes, which may prove to be especially important as Zip Code and other data that is not strictly personal becomes easier to use for personal profiling purposes. Secs. 501-513.

Ironically, the E-Government Act makes no improvements in Congress' own practices -- failing to address such deficiencies as the lack of a searchable index of individual Member voting records.

For more information:

- CDT Deputy Director Jim Dempsey's testimony on FISMA, May 2, 2002 http://www.cdt.org/testimony/020502dempsey.shtml
- CDT's 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
- More on E-Government http://www.cdt.org/righttoknow/

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

CDT POLICY POST
Volume 8, Number 26, November 25, 2002

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

CONTENTS:

---

(1) CDT AND INFODEV PUBLISH E-GOVERNMENT HANDBOOK FOR DEVELOPING COUNTRIES CDT has published a comprehensive resource on e-government for developing and transitional countries. The "E-Government Handbook for Developing Countries" was funded by the World Bank's InfoDev (Information for Development) group.

The Handbook catalogs key resources on e-government in a format readily useful for policymakers in the developing world. Moreover, almost all of the case studies and models are drawn from developing and transitional nations, showing that e-government is not a tool limited to the richer countries.

As used in the Handbook, the concept of e-government means the use of information and communications technologies (ICT) to transform government by making it more accessible and accountable to citizens. Thus, e-government is not achieved merely by putting computers on the desks of government officials. Rather, e-government involves the relationship between the government and its citizens.

A PDF-version of the Handbook is available at:
http://www.cdt.org/egov/handbook/2002-11-14egovhandbook.pdf

The World Bank's infoDev program is at: http://www.infodev.org/

The Handbook was released to coincide with the State Department's Implementing E-Gov Conference -- http://www.marketaccess.org/event_tda_egov.asp -- and infoDev's Symposium 2002 in Chongqing, China -- http://www.infodev.org/symposium2002/

---

(2) HANDBOOK OUTLINES THREE PHASES OF E-GOVERNMENT AND ITS TRANSFORMATIVE POTENTIAL The Handbook is structured around the three phases of e-government:

- **Publish** - putting government information - laws, regulations, forms, data online;
- **Interact** - increasing public participation in government decision-making by enabling the public to interact with government officials;
- **Transact** - allowing citizens to obtain government services or transact business with the government online.

It has been shown that online accessibility of information and services, wisely implemented, can make government more accountable by making its operations more transparent and thus reducing the opportunities for corruption. E-government projects, if structured around existing infrastructure and responsive to the needs of the population, can also serve other development objectives, especially benefiting rural and traditionally underserved communities.

The Handbook also identifies case studies and models illustrating the way in which e-government can transform government, based on five key elements of successful e-government projects:

- **Process Reform** - rather than automating paper-based inefficiencies, e-gov projects should streamline and consolidate offline processes.
- **Leadership** - e-gov succeeds when elected officials or appointed administrators set objectives and push the bureaucracy to adapt.
- **Strategic Investment** - e-gov projects require sustained resources to produce cost-savings.
- **Collaboration** - successful e-gov requires new relationships among government agencies as well as partnerships with NGOs and the private sector.
- **Civic Engagement** - the concept of e-government must revolve around the citizen and citizens should be involved from the outset in designing e-gov programs.

---

(3) ONLINE VERSION HIGHLIGHTS E-GOVERNMENT RESOURCES Some of the most innovative uses of the Internet in governance are appearing in the developing world, as ICTs are being used to streamline government and connect it more closely with the people it is supposed to serve. Our goal in creating the Handbook was to offer concrete guidance to government officials and others in the developing world, presenting for the first time a comprehensive index of e-government models and resources, focused on success stories in the developing world. The Handbook presents a roadmap - in fact, a compilation of roadmaps - for policy-makers considering electronic government as a mechanism for reform.

In building the Handbook, CDT assembled a host of case studies, best practices and other online resources, and drew recommendations from them to illustrate and guide readers through the ideas and concepts of e-government.

The companion online resource contains links to the useful sites and other resources we identified, searchable electronically and categorized by the three phases of e-government, as well as to the various elements of success, challenges and opportunities.

The electronic version of the Handbook is at http://www.cdt.org/egov/handbook/

For information about e-government in the US, see http://www.cdt.org/righttoknow/

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

CDT POLICY POST
Volume 8, Number 27, December 12, 2002

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

CONTENTS:

---

(1) NEW STUDY SHOWS INTERNET FILTERING BLOCKS VALUABLE SITES, BUT CAN BENEFIT PARENTS A new study confirms that filtering technologies can over-block constitutionally-protected speech, but can be effective when used voluntarily in the home by knowledgeable consumers.

The study, "See No Evil: How Internet Filters Affect the Search for Online Health Information," funded by the Kaiser Family Foundation, looked at the ways in which Internet filters impact young people's access to online health information. The study was conducted in response to concerns that Internet filters intended to block young people's access to objectionable material online also prevents them from viewing non-pornographic health information. It provides empirical evidence about over-blocking of material, particularly material about health issues.

The study finds that filtering software works remarkably well at the least restrictive settings, blocking 87% of porn sites but only 1.4% of health-related sites. But at higher settings, filters also block many important health sites on a range of important issues, from mental health to sexually transmitted disease. At the intermediate blocking level, 5% of health-related sites are blocked; at the most restrictive level, 24%. The increase in blocked health content is especially pronounced, the study finds, on searches related to sexual health. For example, for a search on "safe sex," on average about one in ten health sites (9%) is blocked at the least restrictive level of blocking, one in five (21%) at the intermediate level, and one in two (50%) at the most restrictive level.

The Kaiser study is available at http://www.kff.org/content/2002/20021210a/

---

(2) COURTS WERE CORRECT THAT FILTERS BOTH OVER-BLOCK AND UNDER-BLOCK The Kaiser study affirms the findings of the lower federal court in the case challenging the Children's Internet Protection Act (CIPA) about the limitations of filtering technologies - that filters both over-block and under-block speech. The case is now on appeal to the US Supreme Court.

Concerns about young people's exposure to online pornography and other objectionable material led to the passage of CIPA in 2000. The Act requires schools and libraries receiving federal funds to block material that is obscene, child pornography, or "harmful to minors."

The American Library Association, together with library patrons, Web site publishers and a group of libraries challenged CIPA on First Amendment grounds. A panel of federal judges found that thousands of Web pages containing constitutionally protected speech are wrongly blocked by the four leading filtering programs, and that those pages represent only a fraction of Web pages wrongly blocked by the programs. The court found that it is currently impossible, given the Internet's size, rate of growth, rate of change, and architecture, and given the state of the art of automated classification systems, to develop a filter that neither under-blocks nor over-blocks a substantial amount of speech.

The court further found that libraries can exercise less restrictive means to control children's access to objectionable online material, including instituting Internet use policies, enforcing restrictions against accessing illegal speech, and keeping unfiltered terminals that are accessible by children within view of library staff.

The district court decision in the CIPA litigation can be downloaded from http://www.paed.uscourts.gov/documents/opinions/02D0414P.HTM

---

(3) FILTERING REMAINS AN IMPORTANT TOOL WHEN VOLUNTARILY USED BY FAMILIES In CDT's view, there is a world of difference between what parents can choose to do and what the government can mandate. The findings of the Kaiser study, as well as the court in CIPA, affirm CDT's position that filters are important tools when used voluntarily in the home by parents who understand their capabilities and limitations, and who can tune them to reflect their family's values and their developing children's evolving needs. However, the study's findings about over-blocking demonstrate that those same filters, when mandated by government for use in libraries, violate the First Amendment by blocking access to constitutionally protected speech.

Moreover, the study finds that filtering products block a significant amount of pornographic material - at least 87% even when filters are set at their least restrictive level. CDT believes that these figures demonstrate that filters, when knowledgeably applied, are far more effective than any government censorship scheme.

To assist parents and others in understanding the range of filtering technology, CDT has supported GetNetWise, a user-friendly online resource for child protection technology.

GetNetWise is available at http://www.getnetwise.org

For more information about CDT's involvement in challenges to government attempts to censor the Internet, see http://www.cdt.org/speech/

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

CDT POLICY POST
Volume 8, Number 28, December 13, 2002

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

CONTENTS:

---

(1) Homeland Security Department Faces Steep Challenges, Poses Momentous Potential and Risk

The Homeland Security Act signed by President Bush on November 25, 2002 creates the new Department of Homeland Security (DHS) and grants it momentous responsibilities and powers. It is earnestly hoped that DHS will provide needed coordination to government anti-terrorism efforts. The new Department will have wide-ranging authority to compile, analyze, and mine the personal information of Americans. Important issues of oversight and control remain to be addressed. CDT is urging the Administration and Congress (even while in recess) to immediately begin setting out privacy guidelines and oversight mechanisms to ensure that the new department's data analysis activities are focused, controlled and accountable, both for effectiveness in preventing terrorism and for the protection of liberties.

The DHS consolidates 22 separate agencies into a new Cabinet department with 170,000 employees. The components being transferred to DHS include:

- Coast Guard;
- Customs Service;
- Secret Service;
- Immigration and Naturalization Service (INS);
- the recently-formed Transportation Security Administration.

The new Department is structured around four directorates, whose titles give some idea of the agency's

mission and scope:

- Information Analysis and Infrastructure Protection;
- Science and Technology;
- Border and Transportation Security;
- Emergency Preparedness and Response.

The DHS will absorb five components with computer security responsibilities:

- National Infrastructure Protection Center (NIPC) of the FBI http://www.nipc.gov
- National Communications System of the Defense Department;
- Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce http://www.ciao.gov;
- National Infrastructure Simulation and Analysis Center of the Energy Department;
- Federal Computer Incident Response Center (FedCIRC) of the General Services Administration.

Yielding to concerns of the computer industry, the transfer does not include the Computer Security Division of the National Institutes of Standards and Technology.

The combination of NIPC and FedCIRC is noteworthy, in that it combines in one entity the federal computer system intrusion detection activities of FedCIRC and the private sector protection activities of the FBI. If a broader intrusion detection program like the FIDNet system proposed several years ago is to be constituted, this would be the basis for it.

The text and legislative history of the Act are at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.5005:

---

(2) New Department Has Essentially Unlimited Access to Information for Data Mining and Data Analysis The new Department is tasked to "access, receive, and analyze" a wide array of information that includes "law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities."

Strictly speaking, the new Department has no new collection authorities, but many of the components being consolidated into DHS (such as Secret Service, Customs, and INS) have investigative and intelligence collection units of their own. There is no doubt that the new agency will have wiretap authority and other intrusive powers. Moreover, the Department can call upon information for any other intelligence or law enforcement agency. Indeed, when you string together the authorities of the DHS, you get an agency that will help control the collection priorities of other agencies and then be able to access electronically their entire files of undigested intelligence:

- DHS will have a say in deciding what other agencies, including the CIA and the NSA, collect at home and abroad. (Sec. 201(d)(10).)
- DHS can access and receive law enforcement information, intelligence information and other information from Federal State and local government agencies and the private sector.
- Except as otherwise directed by the President, the Department "shall" have access to "unevaluated intelligence." (Sec. 202(a)(1).)
- The Secretary may obtain access "on a regular or routine basis ... [to] broad categories of material, access to electronic databases, or both." (Sec. 202(b)(1).) Broadly read, this means that DHS can have

online access to the files of the FBI, the CIA and the signals intelligence agencies.
- The new DHS is expressly authorized to receive wiretap information and grand jury information collected by any other agency.

The potential scope of this data gathering and analysis is enormous, and both the challenge of analysis and the potential for abuse are apparent. While the Act does provide some structures for safeguarding privacy, rigorous oversight will be needed.

These provisions must be viewed in the context of inadequate privacy protections in law, the enhanced surveillance authorities already granted in the PATRIOT Act and new "data mining" initiatives underway.

The most ambitious and potentially far-reaching of these data mining is known as Total Information Awareness (TIA), a new R&D effort being managed by the Defense Advanced Research Projects Agency (DARPA) to aggregate and analyze information from a wide array of public and commercial databases. The program is just one of a number of government data mining efforts, including the FBI's Trilogy program and the Transportation Security Administration's Computer Assisted Passenger Profiling System (CAPPS II).

Contrary to published reports, there is nothing in the DHS Act directly concerning TIA. TIA was launched before this Act was even drafted, with relatively small amounts of funding in DARPA's budget. TIA is not under the authority of the new DHS. However, it is clear that the results of TIA's research, as well as other similar research being performed by the contractors working for other agencies, will be made available to DHS.

TIA website http://www.darpa.mil/iao/

---

(3) Act Includes Privacy Oversight Mechanisms The DHS Act includes important new oversight mechanisms, including:

- Privacy Officer, a senior official with "primary responsibility for privacy policy" (sec. 222);
- Officer for Civil Rights and Civil Liberties, who shall review and assess information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees and officials of the Department (sec. 705);
- Inspector General, who, unlike IGs in most other agencies, is under the authority, direction, and control of the Secretary and prohibited from investigating matters placed off-limits by the Secretary - these provisions are similar to those applicable to the IG for the Defense Department (sec. 811);
- Citizenship and Immigration Services Ombudsman, who shall assist individuals and employers in resolving immigration problems (sec. 452).

Section 221 of the Act requires the Secretary to "establish procedures" concerning the use of information "shared" under the Act that

- limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;
- ensure the security and confidentiality of such information;
- protect the constitutional and statutory rights of any individuals who are subjects of such information; and
- provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

In addition, the Act includes other provisions intended to protect privacy:

- Prohibition of TIPS - Section 880 expressly states that "any and all activities of the Federal Government to implement the proposed component program of the Citizen Corps known as Operation TIPS (Terrorism Information and Prevention System) are hereby prohibited." TIPS was a proposed program that would have enlisted delivery men and other civilians to report on any suspicious conduct of their customers.
- National ID not authorized - Sec. 1514 states "Nothing in this Act shall be construed to authorize the development of a national identification system or card." That is different from a prohibition.

Other provisions weigh against oversight. Section 871 allows the Department to form advisory committees with industry representatives that are exempt from the Federal Advisory Committee Act (FACA), an open government law that requires open meetings and puts limits on special interests.

---

(4) Privacy Guidelines, Careful Oversight Required While information technology appropriately has a major role to play in preventing terrorism, it is incumbent on the President, the new DHS Secretary and Congress to match expanded information gathering and analysis powers with expanded guidelines and oversight. The creation of a Privacy Office within DHS is one step, but the process also requires the adoption of rules and guidelines that the new office can enforce.

As noted, the Act calls for the adoption of privacy guidelines. In developing these guidelines, attention must be paid to basic questions of fair information practices, including what information is used, who has access to it, what standards of accuracy and timeliness are required, how "hits" will be verified, and how results will be characterized and disseminated. There must be effective audit trails and robust review mechanisms to protect against unauthorized access and inappropriate use of information. Questions to be addressed also include how the government will obtain the data - by compulsory process, by purchase, by subscription, or by voluntary sharing. The analysis must take into account the fact that there are few constraints on government access to records held by private corporations and that the federal Privacy Act imposes few meaningful constraints on the sharing among government agencies of information once it is obtained for national security purposes.

For more information on the use of information technologies and the need for guidelines, see the report of the Markle Task Force on National Security in the Information Age: http://www.markletaskforce.org/

---

(5) FOIA Exemption and Email Disclosure Provisions Also of Concern The Act includes a new FOIA exemption for "voluntarily shared critical infrastructure information" submitted to the new Department. (Sec. 212-215.) The provision, long supported by some IT companies, may limit the ability of small businesses and members of the public to learn about threats and vulnerabilities that affect their computer systems. Under the provision, information about infrastructure vulnerabilities that companies submit to the government must be withheld from disclosure under the FOIA. The new provision goes so far as to make it a crime for a federal official to disclose critical infrastructure information to the public or to affected companies if the disclosure is not "authorized."

Sen. Patrick Leahy (D-VT) called the exemption "the most severe weakening of the Freedom of Information Act in its 36-year history." He said it "would hurt and not help our national security, and along the way it would

frustrate enforcement of the laws that protect the public's health and safety." A more narrowly circumscribed Senate version of the exemption was rejected in favor of a broader House version. However, it should be stressed that the new exemption applies only to information submitted to the DHS. A key question will be whether the exemption actually spurs the increased disclosure of vulnerability information to the government that its proponents promised.

The Homeland Security Act also includes what had been a free-standing bill, the Cyber Security Enhancement Act, which includes a provision undermining privacy online by greatly expanding the ability of ISPs to "voluntarily" disclose information government officials. (Sec. 225.) Under the provision, the contents of email messages or instant messages can be given to any government official in an "emergency" even when there is no factual basis stated for the emergency and there is no imminent threat of injury. CDT's more detailed analysis of the Act is online at http://www.cdt.org/security/homelandsecuritydept/021210cdt.shtml

---

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

CDT POLICY POST
Volume 8, Number 29, December 19, 2002

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

CONTENTS:

Again in 2002, courts grappled with a range of legal disputes involving the Internet. Some of these cases involved constitutional challenges to legislation specifically addressing the Internet, with the courts rejecting Congress' efforts to regulate content on the Internet. Other important cases involved the challenge of applying traditional rules developed offline to the special character of the global digital networks. In the latter situation, often the issue resolved into one of jurisdiction - when could a court exercise jurisdiction over a content creator outside its geographic bounds? A third important category of cases involved privacy and anonymity.

Here is CDT's highly selective listing of the important judicial cases affecting the Internet in 2002 - including some pending before the US Supreme Court and not to be decided until 2003.

- Supreme Court Blocks Enforcement of Federal Law on "Harmful to Minors" Web Content

The Child Online Protection Act (COPA), 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). In 1999, a federal district court held that COPA unconstitutionally burdens speech that is protected for adults and prohibited the Justice Department from enforcing of the statute. That ruling was upheld by the Third Circuit Court of Appeals and the government appealed to the Supreme Court.

In May 2002, the Supreme Court handed down a somewhat inconclusive ruling that kept the injunction in force, blocking the Justice Department from enforcing the Act. The Court returned the case to the appeals court based on flaws in that court's interpretation of the "community standards" obscenity test as applied to the Internet. The appeals court took up the case again on October 29, 2002 and the case is quite likely to go to the Supreme Court a second time in 2003.

The Supreme Court decision on COPA, ACLU v. Ashcroft, is at
http://www.supremecourtus.gov/opinions/01pdf/00-1293.pdf

CDT's "friend of the court" brief after the case went back to the appeals court is at
http://www.cdt.org/speech/copa/020828remandamicusbrief.pdf . For more information, see CDT's May 13, 2002 Policy Post http://www.cdt.org/publications/pp_8.11.shtml

- Federally-Mandated Library Filtering Ruled Unconstitutional

A federal court in Philadelphia rejected as unconstitutional a law that would have required nearly every public library in America to install and use Internet filtering software. The three-judge panel unanimously ruled on May 31, 2002 that the Children's Internet Protection Act (CIPA), passed by Congress in 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. The US Supreme Court has accepted the direct appeal on this case, with briefing set for early 2003.

The lower court decision in the case, American Library Association v. United States, can be found at
http://www.paed.uscourts.gov/documents/opinions/02D0414P.HTM

For more information, see CDT's June 11, 2002 Policy Post http://www.cdt.org/publications/pp_8.14.shtml

---

(2) Privacy Cases Mixed as Secret Surveillance Powers Expanded

- Secretive Appeals Court Permits Wider Use of FISA

A special Foreign Intelligence Surveillance Court of Review ruled on November 18, 2002 that the USA PATRIOT Act gave the Justice Department the authority to use in criminal cases the special and in some ways looser rules created for foreign intelligence investigations. The court, which rejected arguments made by CDT, ACLU and others in a friend of the court brief, nevertheless emphasized that the law still required a finding of probable cause to believe that the target of the surveillance was an agent of a foreign power and was engaged in terrorism or activities in preparation therefore. But oversight is difficult, as many targets are never told they were the subject of surveillance.

The court's decision is online at http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf

CDT's brief, the lower court decision and the government's briefs are available at
http://www.cdt.org/security/usapatriot/implementation.shtml#surveillance

- Supreme Court Again Defends Anonymity

In a case concerning anonymity offline, but with implications for anonymity online and especially for spam, the Supreme Court upheld the rights of Jehovah's Witnesses to go door-to-door to talk about their faith without registering with the town first. The Supreme Court held that a municipal ordinance requiring individuals to obtain a permits with their name on them before engaging in door-to-door advocacy and to produce them upon demand violates First Amendment anonymous speech rights. The case may suggest that states and the federal government would be limited in requiring true name and address on spam, at least spam that is non-commercial.

The opinion in the case, Watchtower Bible and Tract Society v. Village of Stratton, is available online at
http://www.supremecourtus.gov/opinions/01slipopinion.html

- Virginia Supreme Court Requires ISP to Reveal Subscriber ID

On the other hand, the Virginia Supreme Court upheld a lower court decision ordering AOL to reveal information on an anonymous subscriber. The order arose from a libel and unfair business practice claim brought in California over postings on a Yahoo! chat board. Yahoo! complied with an order from the California court and traced the posting to an AOL subscriber, but AOL resisted revealing further information. A Virginia trial court ordered the information revealed on the unfair business practice claim and the state Supreme Court upheld that decision on appeal. The actual holding of the case was fairly narrow, however - that AOL had go to the California court if it wanted to try to quash the subpoena to disclose its subscriber's identity.

The Virginia Supreme Court decision in the case, AOL v. Nam Tai Electronics, is at
http://www.courts.state.va.us/txtops/1012761.txt

---

(3) US Courts Take Narrow View, Some Foreign Courts Take Broad View, of Jurisdiction over Net

- French Blocking Order Against Yahoo! Not Enforceable in US

On December 2, 2002, a US federal appeals court heard oral argument in a case challenging a ruling by a French court that had ordered Yahoo! to block French citizens from accessing Nazi items offered for sale by third parties on Yahoo.com's auction site. The French court directed Yahoo! "to take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes." A lower US federal court ruled in September 2001 that the French order was not enforceable against Yahoo in any US court. The US court determined that enforcement of the French order would violate Yahoo's First Amendment rights. The court of appeals should rule in the first half of 2003.

The case is Yahoo v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168 (N.D. Ca., September 24, 2001).

Appeals court brief by CDT, ACLU, and others in support of Yahoo!
http://www.cdt.org/jurisdiction/020506yahoo.pdf

For more information, see CDT's May 10, 2002 Policy Post http://www.cdt.org/publications/pp_8.10.shtml and http://www.cdt.org/jurisdiction/ where you can find the French court opinion and other briefs

- Australia Courts Claim Jurisdiction Over US-based Website

Allegation that Barron's magazine defamed an Australian citizen through an article posted on the magazine's web site. The High Court of Australia ruled in Glutnick v. Dow Jones & Company, Inc. that Australian courts have jurisdiction over an American publisher in large part because the publisher's website was accessible in Australia. The Australian decision raises serious concerns about Internet free speech internationally.

The Australian decision is at http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.

- US Court Refuses to Extend Long-Arm Jurisdiction Based on Web Site

In a case contrasting with the Australian and French rulings, a US federal appeals court ruled on December 13, 2002 that a Virginia prison warden could not sue two Connecticut newspapers in Virginia court over articles about the conditions in which Connecticut inmates were being held under a contract with a Virginia prison. The articles were posted on the papers' web sites. The appeals court held that the fact that the newspapers' websites could be accessed anywhere, including Virginia, was not by itself sufficient to subject

them to Virginia law. In order to be hauled into court in Virginia, the Connecticut newspapers must have had the "manifest intent of targeting Virginia readers." CDT joined a "friend of the court" brief supporting the publishers.

The appeals court decision in the case, Young v. New Haven Advocate, is at http://pacer.ca4.uscourts.gov/opinion.pdf/012340.P.pdf

---