CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 1, January 9, 2003

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

The 108th Congress, which began its business this week, will face a wide array of issues affecting the Internet. As in past years, it is likely that hundreds of Internet-related bills will be introduced. They will run the gamut from those that would advance privacy and the principle of user control to those that will pose threats to openness and other civil liberties online. It is impossible to predict what will be enacted before Congress adjourns in 2004 just before the presidential election, but here is CDT's overview of some key issues likely to receive serious consideration. We also take a look back at the 107th Congress (2001-02), when landmark legislation was enacted.

- Digital Rights Management

A critical debate resumes in Congress about how to protect copyrighted material in the new digital media -- a debate that could define how Americans watch TV, listen to music, and use their computers for years to come. Last year, the proposals - none of which passed - ranged from the Hollings bill on digital rights management, to the Berman bill on peer-to-peer file sharing, to the Boucher proposal to amend parts of the Digital Millennium Copyright Act (DMCA). Rep. Rick Boucher (D-VA) has already reintroduced his DMCA bill this week (H.R. 107).

For more on these issues: http://www.cdt.org/copyright/.

- Terrorism, Surveillance and Privacy

There have been rumblings about a PATRIOT Act II, which could propose further expansions of government surveillance power. Meanwhile, Congress should be pursuing oversight of the first PATRIOT Act. Much of the implementation of that law, particularly as it affects privacy, is shrouded in secrecy and gag orders.

Congress also should have its hands full overseeing creation of the new Department of Homeland Security (DHS). The House Republican leadership has announced a new select committee for oversight of homeland security issues. CDT is urging the Administration and Congress 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 civil liberties.

Sen. John Edwards (D-NC) has proposed creating a new domestic intelligence agency to take over the FBI's duties to collect intelligence within the United States. Sen. Edwards has emphasized that particularly intrusive investigations by such an agency should be subject to special controls.

The question of a national ID card will come up in the context of proposals to standardize features of state drivers' licenses, which will be debated in a bill reauthorizing federal highway funding.

Sen. Edwards' views on the topic: http://edwards.senate.gov/speeches/2002/homeland_12-18.html CDT's recent Policy Post on DHS: http://www.cdt.org/publications/pp_8.28.shtml. Resources on terrorism issues: http://www.cdt.org/security/010911response.shtml

- Consumer Privacy

The US still lacks baseline federal legislation to protect consumer privacy. Online and offline privacy issues are expected to come up in the course of the reauthorization fight over the 1996 amendments to the Fair Credit Reporting Act, which sunset at the end of 2003. Sen Richard Shelby (R-AL), incoming chairman of the Banking Committee, has said that he favors stronger privacy protections for financial data and opposes preemption of state laws. Sen. John McCain (R-AZ), chairman of the Senate Commerce Committee and author of an opt-out proposal in 2000, is also expected to address privacy issues, beginning with possible hearings this year.

See: http://www.cdt.org/privacy/

- E-Government

A landmark e-government law was enacted last year (see below), but it failed to address gaps in Congress' own online resources. In 2003, there may be a move to put more Congressional material online.

More on access to government information online: http://www.cdt.org/righttoknow/

- Spam

Once again, the last Congress failed to pass spam legislation, even though bills were approved at the committee level in both House and Senate. The "Controlling the Assault of Non-Solicited Pornography and Marketing" Act (the "CAN-SPAM" Act or S. 630) sponsored by Senators Conrad Burns (R-MT) and Ron Wyden (D-OR) passed out of the Senate Commerce Committee in May 2001 and the Unsolicited Commercial Electronic Mail Act (H.R. 718), sponsored by Rep. Heather Wilson (R-NM), was reported by both the Commerce and Judiciary Committees in the House, but neither received Floor consideration. The Direct Marketing Association announced in October 2001 that it would support federal anti-spam legislation as a method of helping legitimate marketers.

- Other issues

Other issues range from the Internet tax moratorium to virtual child pornography, identity theft, online gambling, and Internet censorship in repressive regimes. A bill introduced this week by Senate Democrats, the Justice Enhancement & Domestic Security Act (S. 22), includes provisions on child pornography online and provisions designed to protect against misuse of Social Security numbers and mitigate the harm to individuals victimized by ID theft.

(2) 2001-02 Saw Momentous Legislation Affecting Digital Privacy, E-gov

- Government surveillance

The most momentous piece of legislation adopted by the last Congress (2001-02) was the USA PATRIOT Act, signed into law on October 26, 2001. The Act dismantled many privacy protections for communications and personal data.

Resources on the PATRIOT Act and other anti-terrorism measures can be found at http://www.cdt.org/security/010911response.shtml.

For a journalistic account of the passage of the PATRIOT Act , see "Six Weeks in Autumn," by Robert O'Harrow, The Washington Post Sunday magazine, Oct. 27, 2002
http://www.washingtonpost.com/wp-dyn/articles/A1999-2002Oct22.html

- Information analysis

Nearly as important, the Homeland Security Act signed by President Bush on November 25, 2002, created the new Department of Homeland Security (DHS) and granted it momentous responsibilities and powers. The DHS, which comes into existence on January 24, will consolidate 22 separate agencies into a new Cabinet department with 170,000 employees. It will have wide-ranging authority to compile, analyze, and mine the personal information of Americans.

CDT's December 13, 2002, Policy Post on the Homeland Security Act:
http://www.cdt.org/publications/pp_8.28.shtml.

- E-Government

The E-Government Act of 2002 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.

CDT's November 21, 2002 Policy Post on the E-Gov Act: http://www.cdt.org/publications/pp_8.25.shtml.

- Communications Privacy

The Cyber Security Enhancement Act, incorporated into the homeland security bill, 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 without a court order 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 Cyber Security Enhancement Act is online at
http://www.cdt.org/security/homelandsecuritydept/021210cdt.shtml.

- Domain Names

A law was passed mandating creation of a ".kids" space within the ".us" Internet domain. Content in ".kids.us" is required to be age appropriate for children under the age of thirteen, and linking to domains outside ".kids.us" is prohibited. CDT and others raised serious questions about ".kids.us" as increasing government involvement in setting online content standards.

The text and legislative history can be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03833:

For CDT's position: http://www.cdt.org/dns/020912dotkids.shtml.

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

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_9.01.shtml.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 2, January 14, 2003

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

(1) Broad Coalition Calls For Moratorium, Hearings On Datamining A broad coalition of public interest organizations sent a letter to Congress yesterday (1/14/03) asking for a moratorium on the Defense Department's Total Information Awareness (TIA) program until key questions about the "datamining" initiative have been answered.

CDT joined the ACLU, Americans for Tax Reform, and other groups in sending a letter to the chairs and ranking members of four congressional committees, urging that Congress put the brakes on TIA and similar datamining operations until officials have demonstrated the technique's effectiveness and explained how it will be controlled to protect privacy.

The federal government already has invested $128 million in TIA, but very little is known about how it works and whether Americans' privacy is being protected. In particular, the letter seeks information about the sources of the information used by TIA and similar programs; the datamining applications already developed and sent on to federal agencies; the uses of any information generated by TIA or similar datamining programs; and how errors in the data or applications might affect innocent Americans.

The organizations signing the letter include: CDT, the American Civil Liberties Union; American Conservative Union, Americans for Tax Reform; the Center for National Security Studies; the Eagle Forum; the Electronic Frontier Foundation; the Electronic Privacy Information Center; and the Free Congress Foundation.

The coalition's letter and other materials on datamining are available at
http://www.cdt.org/security/usapatriot/implementation.shtml#surveillance

(2) Senators Raise Questions About TIA Last Friday (1/10/03), three Senators requested detailed information from Attorney General Ashcroft about the Justice Department's use of datamining. The letter from Senators Leahy (D-VT), Feingold (D-WI) and Cantwell (D-WA) requested detailed information about ongoing datamining operations underway within the Justice Department, including details about where the Department is getting its information, whether it is relying on any safeguards to ensure the reliability of that data, and whether it views the Privacy Act as imposing any restrictions on its datamining activities. The Senators also asked about the Justice Department's work with the Total Information Awareness project.

The letter further seeks justification for the seemingly redundant Foreign Terrorist Tracking Task Force, a new Justice Department entity that maintains its own "lookout list" and conducts intelligence analysis -- despite the fact that the FBI already keeps a Terrorism Watch List and has an Office of Intelligence established to gather and analyze counter-terrorism intelligence.

Finally, the Senators' letter asks whether the Justice Department intends to transfer its datamining operations to the new Department of Homeland Security, the one agency statutorily tasked with integrating information from various sources.

The Leahy/Feingold/Cantwell letter is also at
http://www.cdt.org/security/usapatriot/implementation.shtml#surveillance

---

(3) Datamining Unproven; Scope Undefined, Legal Basis Unclear, Guidelines Lacking It is entirely desirable that the federal government make effective use of information technology to prevent terrorism. However, information collection and analysis proposals, like any other anti-terrorism measure, must be subject to scrutiny and control at two levels:

- Will the proposed measure be effective?
- Can the proposal be implemented in a way that is consistent with Constitutional principles? (In the case of information systems, how can the measure avoid unfairness, mistake and undue intrusions on privacy?)

One of the most controversial information technology applications being proposed in the fight against terrorism involves the technique known as "datamining" - which includes the broad scanning of personal data in government and private sector databases looking for patterns that might offer predictions of terrorist conduct.

The federal government's use of datamining could grow dramatically. The new Department of Homeland Security will be a center for analysis of data from a wide range of sources. Also, in addition to the Pentagon's TIA office, the FBI with its Trilogy program and the Transportation Security Administration through its Computer Assisted Passenger Profiling System (CAPPS II) are developing new abilities to retrieve and analyze information maintained in their own databases and in the databases of other government agencies and private companies.

There is growing concern in Congress that these proposals are being pursued before resolving key questions about scope, effectiveness, and legality. For example, how will the government obtain the data - by compulsory process, by purchase, by subscription, or by voluntary sharing?

Even if the effectiveness of datamining is demonstrated, access to non-public information should not proceed until guidelines have been developed to govern the collection, retention and dissemination of information.

Attention must be paid to

- what information will be used,
- who will have access to it,
- what standards of accuracy and timeliness will be applied,
- how will "hits" be verified,
- how will results be characterized and disseminated,
- how will individuals be able to correct mistakes.

There also should be effective audit trails and robust review mechanisms to protect against unauthorized access and inappropriate use of information.

An initial discussion of these issues is found in the report of the Markle Task Force on National Security in the Information Age: http://www.markletaskforce.org/

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

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_9.02.shtml.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 3, January 23, 2003

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

(1) Feds Open Portal for Online Comments on Regulations In a step forward for e-government, the Bush Administration today unveiled a new web site, http://www.regulations.gov, that allows individuals to more easily find and comment on proposed rules being considered by federal agencies.

Increasingly, government agencies have been accepting online comments opposing or supporting proposed regulations, and a 1998 law requires all agencies, "when practicable," to accept submission of online comments by October of this year. But in the past, citizens had to know what agency might have responsibility for an area of interest. The new regulations.gov web site allows Internet users to search by keyword across government agencies for areas of interest, rather than having to guess which agency is writing a particular regulation.

The site also creates a common interface for filing comments. Agencies generally have different rules about what kind of information they want from persons submitting comments and different formatting styles. The new web site automatically provide submitters with the proper fields needed to submit comments to all covered agencies.

(2) Improvements Needed in New Site While the introduction of regulations.gov is a positive step, its creators intend to improve it over time. Here are some immediate improvements CDT is recommending.

- The search engine should be augmented with various browsing functions. While one of the main benefits of the site is the ability to search by keyword across departments and break down the "stovepipes" that have traditionally made government bureaucracies practically obscure, the current search tool may not be of much use if an individual does not know the exact terminology for a regulation. Browsing tools can be the only way for individuals not steeped in policy terminology to find a particular rule for comment. The site creators say that they plan to implement browsing features gradually.

CDT believes that there are some helpful browsing features that could easily be added to the site immediately to assist citizens who are not experts in any particular field. Specifically, the site should include:

- A "New Today" feature (similar to the existing Federal Register Table of Contents, but focused only on proposed regulations).
- A "Closing This Week" section that would serve as a reminder of comment periods that are ending soon.
- A "Hot Topics" section listing a few proposals that are especially important or are of broad public interest.

- Also useful, and something the sponsors of the site say that they envision, would be a means for individuals to read the comments of others. If well-designed, this feature could allow for a new kind of interaction between individuals similar to town hall meetings. (If poorly-designed, this feature could also turn comment periods into "flame wars" familiar to all Usenet and chat room participants.) CDT believes that this would be a worthwhile experiment for government to try to improve participatory democracy using online tools.
- Finally, we note that the comments are limited to 4000 characters - a limitation that seems unnecessary, and that basically would seem to create two tracks for filing comments: regulation.gov for non-professionals versus other electronic means, including agency web sites, for businesses, their lawyers and other experts, whose comments frequently exceed 4000 characters.

Ironically, the new site also shines a light on agencies that are not yet accepting comments online. A quick search today showed that the Copyright Office of the Library of Congress, the Drug Enforcement Administration, and the Air Force, among others, do not accept comments online. This should change, both as the site itself brings pressure on agencies to improve and as the upcoming October deadline approaches.

---

(3) Background on Online Rulemaking and E-government Public comments on proposed government regulations are an important part of the democratic process -- in the United States, the concept of federal "notice and comment" rulemaking was a major reform of the first half of the 20th century. While agencies should not make decisions based solely on the referendum of pro and con comments, the comment process remains the most important tool that individuals have to influence the often opaque exercise of power by regulatory agencies in Washington.

In practice, citizen participation in rulemaking has been low, in part because the information was available only in the Federal Register in printed form. As the Federal Register has gone online, and as federal agencies themselves have posted proposed rules on their own agency web sites, a greater number of individuals have been able to participate in the comment process. The Pew Internet & American Life Studies have shown that Americans see commenting on government rules and regulations as a top priority for e-government, and 60% of Americans (75% of Internet users) say that the Internet is the first place that they now look for government information.

Congress recognized the importance of allowing individuals to interact with government online when it passed the Government Paperwork Elimination Act (GPEA) of 1998 requiring agencies to create means for individuals to submit information electronically by October 21, 2003. The E-Government Act of 2002 reaffirmed the obligation.

Yet, the move online has created varying means for individuals to submit comments. To this day, some agencies do not provide web interfaces or accept email or even fax. The rules for submission vary even if the comments are on similar or related topics. For example, the FTC and FCC recently had two different sets of rules for submission of comments on proposed telemarketing "Do Not Call" lists.

E-gov resources and background information:

Federal Register online: http://www.access.gpo.gov/su_docs/aces/fr-cont.html

Pew Internet & American Life study on e-gov: http://www.pewinternet.org/reports/toc.asp?Report=80

CDT's e-government page: http://www.cdt.org/righttoknow/

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

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_9.03.shtml.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 4, February 5, 2003

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

(1) Congress to Decide Fate of DoD Data-Mining Program Congress is now facing a key decision about the Pentagon's development of a massive tool to "mine" the data of innocent Americans looking for suspicious conduct - the Total Information Awareness (TIA) program.

Last month, the US Senate adopted an amendment ("the Wyden amendment") holding up deployment of TIA until basic questions are answered about its potential for error and abuse of privacy. But the amendment hasn't passed the House yet, and the Pentagon has begun to lobby against it.

CDT has set up a special web page where concerned citizens can find out who their Members of Congress are, with phone numbers, to call them and urge them to put some limits on TIA until basic questions about its effectiveness and privacy implications are answered.

The web site is http://www.cdt.org/action/tia/.

(2) What is TIA and What Is Congress' Role? TIA is a Defense Department research project aimed at developing broad sweeps of commercial data, such as credit card records, store purchases, travel records, Internet logs, and medical data - billions of bits of information about the legal activities of innocent people. The idea is to "mine" this data searching for suspicious patterns that may indicate possible terrorists. It could aid investigators if it worked, but so far no one has explained how to avoid errors that can result in people mistakenly being flagged as "terrorists" - and thereby subject to false arrests or being denied jobs because their credit card usage - or their housemate's credit card usage or the credit card usage of someone with a similar name - was suspicious.

CDT and many other privacy groups have raised concerns about the program, urging a moratorium on deployment of it against US citizens until basic questions can be answered. Better use of information in public and private databases is clearly needed to help prevent terrorism, but so far there are no guidelines on what data will be used, under what standards it will be accessed, how long it will be kept, how people will correct mistakes that could damage their employment opportunities, etc.

In January, the Senate passed the Wyden Amendment (sometimes referred to as "Amendment # 59") blocking use of the TIA program unless Congress specifically authorizes it after the Administration submits a report the amendment requires about the program and its effect on privacy. The amendment was added to the omnibus continuing appropriations act, the massive spending bill for fiscal 2003, which passed the Senate on January 24.

The Wyden amendment and other materials about TIA are online at:
http://www.cdt.org/security/usapatriot/implementation.shtml#surveillance

---

(3) Next Step - The House Senate Conference Now Under Way The Wyden amendment has passed the Senate, but not the House. The next big challenge is to preserve the amendment "in conference." The Senate bill must be reconciled with a House-passed spending bill that contains no provision on TIA. The House has appointed some of its senior Members to meet with senior Senators and work out the differences between the two bills. There is pressure to do this quickly, as the fiscal year is already 3 1/2 months old.

To find out what you can do, go to http://www.cdt.org/action/tia/. You can find out who is your Representative in the House and how to express your views on this important issue.

Forward this message (through Friday, February 14, 2003) to other individuals interested in protecting privacy and responding effectively to terrorism.

Many experts recommend calling Congressional offices rather than sending an email or fax. Studies have shown that personal phone calls by informed voters are by far the most effective way to make a difference over a short period of time. By the time the office reads your email, fax or letter, it will probably be too late to have an impact.

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

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_9.04.shtml.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 5, February 1, 2003

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

(1) Senators Re-introduce Resolution To Put More Congressional Info Online Congress, having passed a major e-government act for the Executive Branch and the courts last year, is still lagging in its own use of the Internet to make information available to citizens. Legislation being introduced today could change that.

Led by Sens. John McCain (R-AZ) and Patrick Leahy (D-VT), a bi-partisan group of Senators are today introducing a resolution to put Congressional Research Service reports and lobbying disclosure records online.

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

CRS reports would be useful to researchers, students, librarians, government employees, and ordinary citizens. The McCain-Leahy resolution would put almost 3000 of these reports on the Internet.

The resolution mirrors one introduced two years ago, but stands a better chance of success now. Two years ago, the proposal drew early opposition from the Senate Rules Committee, which has jurisdiction over the matter, and key members were focused on other important issues such as voting reform and campaign finance. Those issues were resolved in the last Congress and thus no longer stand in the way of this proposal. Most importantly, perhaps, the new Chair of the Rules Committee, Sen. Trent Lott (R-MS), co-sponsored the resolution in the last Congress and is expected to support it again.

For more info on e-gov: http://www.cdt.org/righttoknow/

As soon as the bill has a number, we will link to it under "e-gov" at http://www.cdt.org/legislation/

(2) Congressional Research Service Reports Still The Most Wanted Forcing citizens to obtain CRS reports by mail rather than online is one example of Congress' continuing failure to take full advantage of the democratic potential of the Internet.

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

While much of the information that was identified in 1999 has since gone up online, important Congressional information is still not available on the Internet. In the CDT/OMB Watch survey, CRS reports were the #1 most wanted set of documents government-wide. Two other important sets of Congressional information -- the full text of all Congressional hearings and a searchable database of Congressional votes -- also are still not online.

A new report by the Project On Government Oversight (POGO) reconfirms the findings from the CDT/OMB Watch report of 4 years ago. Key points in the new POGO report include:

- CRS's products and its Website, funded with taxpayer dollars, are not readily available to the public. Furthermore, as a Congressional entity, CRS is not subject to the Freedom of Information Act. CRS does not answer direct public inquiries.
- Former Members of Congress, many of whom become lobbyists, can request current CRS publications and limited reference assistance. Therefore, entities such as corporations and universities, which can afford these lobbyists, have access to current CRS publications that public interest groups and the general American public do not.
- CRS has already created a Website at http://www.crs.gov that could be made readily available, so cost is not an impediment to openness.

In addition to urging that CRS products be made readily available to the general public, POGO recommends that the Library of Congress should expand the public THOMAS website to include other information related to the legislative process.

The full POGO report is available at: http://www.pogo.org

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

CDT POLICY POST

Volume 9, Number 6, February 20, 2003

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

(1) CDT Reports Calls Pennsylvania Blocking Law Unconstitutional and Unsound The Center for Democracy and Technology released a major report calling unconstitutional a recent Pennsylvania law that forces Internet Service Providers (ISPs) to block access to numerous web sites without adequate court oversight. The report's release coincides with a request under Pennsylvania's right-to-know law seeking records of the Attorney General's previously undisclosed demands to block web sites pursuant to the law.

The CDT report - entitled "The Pennsylvania ISP Liability Law: An Unconstitutional Prior Restraint and a Threat to the Stability of the Internet" - analyzes a 2002 Pennsylvania law that forces ISPs to block access to any web site deemed "child pornography" without notice to the site's publisher and without any opportunity to challenge the determination. ISPs are required to block the sites even if they do not host the content and have no relationship whatsoever with the publishers of the content. The Pennsylvania Attorney General has since gone even further, bypassing the law's inadequate court procedures to simply demand by letter that sites be blocked. The report argues that the statute, which blocks access to sites that are wholly innocent, is an unconstitutional restriction on speech, blocks access to sites that are wholly innocent.

CDT's report is available at http://www.cdt.org/speech/030200pennreport.pdf.

(2) Background on the Penn. Web Blocking Law Passed in early 2002, the Pennsylvania ISP Liability Law imposes potential liability on ISPs for child pornography available on the Internet, even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content. Essentially, the law makes any ISP doing business in Pennsylvania potentially liable for content anywhere on the Internet.

Under the law, the state Attorney General or any county district attorney can apply to a local judge for an order declaring that (a) certain content on the Internet is probably child pornography, and (b) the content can be reached through the services of a specified ISP. The entire court proceeding occurs with the participation of just the government, with no prior notice to the ISP or the web site owner required, and no notice after the hearing to the web site owner. This kind of proceeding contrasts with typical court proceedings that require notice to parties and an opportunity for both sides to be heard.

Under the law, a judge does not make any final determination that the challenged content is child pornography; instead, the judge needs only to find that there is "probable cause" evidence of child pornography. Based on this determination, the state Attorney General notifies the ISP in question. The ISP then has five days in which to block all access to the specified content, or else face criminal liability.

Critically, the ISP Liability Law imposes potential criminal liability for content that is rely "accessible through" an ISP's or access provider's service. The law lacks any requirement that the ISP have any connection to or responsibility for the content (such as if the content were created by the ISP or one of the ISP's customers). Instead, the potential liability is created simply because - as with any Internet service provided by any ISP - someone in Pennsylvania can reach content located anywhere on the Internet.

---

3. Laudable Goals, Serious Constitutional and Technical Problems While acknowledging the grave nature of the problem of child pornography, CDT's report details the serious problems - both legal and technical - inherent in the law and the Attorney General's actions:

- CDT concludes that the law violates constitutional principles of free speech and due process, and is unconstitutional under both the First and Fourteenth Amendments of the U.S. Constitution.
- Because ISPs must block web sites based on their numeric "Internet Protocol" (IP) address, the law also blocks web sites that are completely unrelated to any child pornography sites, simply because most Internet web sites today share their IP addresses with many other wholly unrelated web sites.
- Because of how the Internet is structured, Pennsylvania's blocking orders reach far outside of the state and prevent people across the country from accessing lawful Internet content.
- The Pennsylvania law forces ISPs to manipulate the sensitive "routing tables" used to send communications around the Internet, increasing the risk of major Internet service outages.
- The law does nothing to remove the child pornography at its source or to prosecute the creators and posters of the content. The law merely attempts to shield Pennsylvania citizens from the content while allowing children to continue to be victimized in the production of the child pornography.

The magnitude of over-blocking under the Pennsylvania law is demonstrated in a separate report - also released this week - by Benjamin Edelman of the Berkman Center for Internet & Society at the Harvard Law School. In that report, Edelman finds that more than two-thirds of all .COM, .NET, and .ORG web sites share their IP addresses with at least fifty other web sites. Any blocking order aimed at one of those web sites under the Pennsylvania law would block all fifty (or more) sites, even if those sites are wholly unrelated to the targeted web site.

In light of these findings, the effect of the law is like stopping mail delivery for an entire apartment building because one tenant is accused of wrongdoing. The law will prevent many Internet users around the country from accessing hundreds or perhaps thousands of innocent web sites, with no notice or explanation whatsoever.

Benjamin Edelman's report, entitled "Web Sites Sharing IP Addresses: Prevalence and Significance," was released by Mr. Edelman this week, and is available at http://cyber.law.harvard.edu/people/edelman/ip-sharing/.

---

4. Request Filed for Records of Undisclosed Web Site Blocking In conjunction with the release of its report, CDT has also assisted in the filing today of a Pennsylvania "Right to Know" Request to the Attorney General, demanding that he disclose the hundreds of web sites that he has blocked since the law went into effect. Professor Seth Kreimer of the University of Pennsylvania Law School, with CDT as counsel, submitted the "open records" request seeking all orders and notices served pursuant to the law on ISPs by the Attorney General's office.

Under Pennsylvania's open records system, the Attorney General must produce the requested documents within ten days. CDT will post the response on our Web site when we receive it.

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

This document may be redistributed freely in full or linked to http://www.cdt.org/publications/pp_9.06.shtml.

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

CDT POLICY POST
Volume 9, Number 7, March 6, 2003

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

(1) CDT Releases Compendium of Papers On Consumer Privacy The Center for Democracy and Technology is today releasing a compendium of papers that examine key issues in the consumer privacy debate. The resource, entitled "Considering Consumer Privacy: A Resource for Policymakers and Practitioners," contains 23 papers by a balanced array of industry representatives, privacy experts and consumer advocates.

Contributors include Chris Jay Hoofnagle of EPIC on access, Pat Faley of the Direct Marketing Association on notice, and NY State Attorney General Eliot Spitzer on preemption.

The compendium comes at a key point in the privacy debate. Over the last year, the privacy landscape underwent significant change. The decline in the dot.com economy prompted a re-examination of the business models and information collection practices of online marketers. The aftermath of September 11 intensified government interest in access to and analysis of consumer data. Rather than pushing privacy aside, these developments led to a more in-depth focus on specific, practical aspects of privacy - notice, choice, access, privacy enhancing technologies, self-regulation, and the respective roles of the states and the federal government.

Congress is likely to return to the debate again this year (see below), against the backdrop of extensive activity at the state level. To inform the process with experience garnered over the last several years, CDT called for papers from experts with a variety of perspectives.

The result should offer Members of Congress, their staffs and the wider public a deeper and more comprehensive understanding of the privacy issue.

"Considering Consumer Privacy: A Resource for Policymakers and Practitioners" can be found at http://www.cdt.org/privacy/ccp/.

(2) Rep. Stearns to Reintroduce Privacy Bill in House Rep. Cliff Stearns (R-FL) is expected, as soon as today, to reintroduce his consumer privacy bill in Congress. Based on Rep. Stearns comments last month, the bill is likely to be similar to the Consumer Privacy Protection Act that he introduced last year.

While the bill addresses several elements of privacy, including notice, choice and security, in crucial respects the bill's language limits the scope or effectiveness of the protections it addresses:

- Sensitive Information - This bill makes no special provisions for financial, medical, political and racial information. Consumers have expressed major concerns about the use of this kind of information as the basis of decisions made about them by businesses.
- Enforcement - The bill leaves all enforcement to the Federal Trade Commission (FTC). Existing privacy law has relied upon the state attorneys general and the rights of private citizens to sue as their main enforcement mechanism.
- Consumer Access - Existing privacy laws and self-regulatory codes of practice generally give the consumer some kind of access to personal information held by a company. The Stearns bill as previously introduced would have taken a major step backward by not requiring a company to give consumers the opportunity to review their own information to determine its accuracy and to make appropriate corrections.

The bill also omitted crucial privacy protections, including effective use limitations, and included over-broad language to preempt state law.

Representative Stearns also said recently that the new bill would include provisions on spam and the use of social security numbers.

Proposed federal privacy legislation introduced in Congress is available at http://www.cdt.org/legislation/108th/privacy/

CDT's analysis of the Stearns bill as introduced in the last Congress is available at: http://www.cdt.org/legislation/107th/privacy/020517stearns.pdf

CDT's comparison of the Stearns bill with the Hollings (D-SC)/Stevens (R-AK) privacy bill from the 107th Congress is available at: http://www.cdt.org/legislation/107th/privacy/comparison.shtml

---

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

CDT POLICY POST
Volume 9, Number 8, March 20, 2003

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

---

(1) New CDT Report Shows How Spammers Can Get Your E-Mail Address A new report from the Center for Democracy & Technology entitled "Why Am I Getting All This Spam?" sheds some light on one of the Internet's most pressing issues -- unsolicited commercial e-mail, a.k.a. spam.

Armed with lists of e-mail addresses, "spammers" send billions of e-mail messages every day, mostly to users who don't want them. As it mounts up, this spam inconveniences tens of millions of Internet users and imposes huge costs on ISPs.

Part of what has made spam such a difficult issue is that it's often impossible to tell how a spammer acquired a user's e-mail address. To address this, CDT embarked on a project to begin to determine the source of spam. We set up hundreds of single-use e-mail addresses and posted or disclosed them on Web sites and newsgroups, and to a variety of corporate and organizational online service providers.

It should come as no surprise to most e-mail users that many of the addresses CDT created for this study attracted spam (nearly 9,000 spam messages in all), but it is interesting to see the different ways that the addresses attracted spam depending on where the e-mail addresses were placed.

The project's results offer Internet users some insight about how certain online behaviors can result in spam, as well as tips to help users reduce the spam that they receive.

"Why Am I Getting All This Spam?" is available at http://www.cdt.org/speech/spam/030319spamreport.shtml [HTML] http://www.cdt.org/speech/spam/030319spamreport.pdf [PDF]

Additional information about spam, and the policy issues associated with it, is available at http://www.cdt.org/speech/spam/

(2) Spam "Harvesters" Target Web Sites, Newsgroups Over 97% of the spam we received was delivered to addresses that had been posted on public Web pages. Spammers use software harvesting programs such as "robots" or "spiders" to record e-mail addresses listed on Web sites, including both personal Web pages and institutional (corporate or non-profit) Web pages. These programs scour the code of Web pages looking for anything that looks like an e-mail address. When they find one, they add it to a list for future spamming.

Spammers' use of harvesting programs is not limited to Web pages. We found that they are also used to siphon e-mail addresses from the headers of postings to USENET newsgroups. We received spam to 85% of the addresses we used to post on USENET.

In order to understand how these harvesting programs work, we tested two methods of "obscuring" e-mail addresses to prevent their harvesting. We found that be posting an address in "human-readable" form -- i.e., the address "user@example.com" could be written "user at example dot com" -- or in HTML-obscured form -- a form that Internet browsers can read, but harvesting programs can't, i.e. "user@example.com" becomes "&#117;&#115;&#101;&#114;&#064;&#101;&#120
;&#097;&#109;&#112;&#108;&#101;&#046;&#099;&#111;&#109;" -- is an effective way to avoid spam. None of the obscured addresses we used in our postings, either on Web pages or in USENET postings, received a single piece of spam.

As technology advances, harvesters may gain the ability to see through these methods of obscuring an e-mail address. For the time being, obscuring is an effective way to avoid spam.

(3) Privacy Policies and Exercising Choice Can Help Users Limit Spam Our project also examined whether disclosing an e-mail address to popular Web companies and other organizations could lead to an increase in spam. We also looked at whether "opting-out" of e-mail from these Web sites would have an impact on the amount of e-mail received by an e-mail address. We found that both privacy policies and "opt-outs" can play an important role in helping users control the amount of spam they receive.

Many of the Web sites to which we disclosed e-mail addresses had posted policies describing how those addresses would be handled, including whether they would be shared with third parties, used for marketing purposes, or other important details. While the terms of the policies we encountered varied, we found that almost all sites followed the policies they had posted on their Web sites. Users who are concerned about spam should review the privacy policies of any Web sites to which they consider disclosing their e-mail address.

In addition, when users were offered the opportunity to "opt-out" of future e-mail communications, that choice was respected in the majority of cases. In most cases, within a few days of "opting-out" of future communications for a given e-mail address, the flow of e-mail to that address stopped. There were, however, a few instances in which we tried to "opt-out" of future e-mail communications to a certain e-mail address, only to have the flow of spam continue.

More information about these exceptions and additional data from the project are available in our report, "Why Am I Receiving All This Spam?".

(4) Tips for Avoiding Spam Currently there is no foolproof way to prevent spam. Based on our research, we recommend that Internet users try the following methods to prevent spam:

1. **Disguise e-mail addresses posted in a public electronic place.** Users can prevent their e-mail addresses from being "harvested" by obscuring it, either in the "human-readable" (user at example dot com) or the "HTML-obscured" ("user@...) methods.
2. **Read carefully when filling out online forms requesting your e-mail address, and exercise your choice.** If you don't want to receive e-mail from a Web site operator, don't give them your e-mail address unless they offer the option of declining to receive e-mail and you exercise that option.
3. **Use multiple e-mail addresses.** When using an unfamiliar Web site or posting to a newsgroup, establish an e-mail address for that specific purpose. This can make it easy to shut off any address that is attracting spam. A number of Web sites now offer "disposable e-mail addresses" that will help you do this.
4. **Use a filter.** Many ISPs and free e-mail services now provide spam filtering. While filters are not perfect, they can cut down tremendously the amount of spam a user receives.
5. **Short e-mail addresses are easy to guess, and may receive more spam.** At least one spammer tried to guess the e-mail addresses used in this study by sending mail to every possible address on our system (a@example.com, b@example.com, c@example.com, etc.). Other spammers may use "dictionary" attacks that try to combine common names or initials in order to guess e-mail addresses. Such techniques are more likely to result in spam when e-mail addresses are short or use common words. E-mail addresses need not be incomprehensible, but a user with a short or common name may want to modify or add to it in some way in his or her e-mail address.

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

CENTER FOR
DEMOCRACY
&
TECHNOLOGY

CDT POLICY POST

Volume 9, Number 9, April 28, 2003

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

---

(1) CDT Report Analyzes Public Policy Concerns About ENUM Technology ENUM, a technology protocol that may provide a critical tool in the more widespread adoption of "voice over the Internet" services, also poses risks to privacy.

CDT's Standards, Technology & Policy Project has issued a report analyzing a range of privacy and other public policy concerns raised by the ENUM protocol. The report sets out detailed policy recommendations that should be followed by national governments and service providers in any implementation of ENUM.

"ENUM: Mapping Telephone Numbers onto the Internet -- Potential Benefits With Public Policy Risks" is available at http://www.cdt.org/standards/enum/ [HTML] and http://www.cdt.org/standards/enum/030428analysis.pdf [PDF].

Additional information about CDT's Standards Project is available at http://www.cdt.org/standards/.

---

(2) What is ENUM and Has it Been Deployed Yet? ENUM is a protocol that allows the translation of normal telephone numbers into a format that can be used to store and retrieve Internet addressing information, which can in turn be used to route communications over the Internet. With ENUM and "Voice over Internet Protocol" ("VoIP") technology, an increasingly amount of voice communications can be carried over the Internet instead of over the traditional telephone network. Initially, ENUM is likely to be deployed by corporations and other large institutions that seek to reduce their use of traditional telephone services (especially international and other long distance service). This technology has the potential to allow users -- corporations and individuals -- to save money and increase the choices they can exercise in their communications.

ENUM will facilitate the routing of telephone calls over the Internet, in a manner that is seamless to the end users. To place a call with ENUM, (1) a person dials a standard phone number on a normal telephone (or on a telephone-like device connected to a computer), (2) the computer or telephone system uses ENUM to check if the called number can be reached over the Internet using VoIP technology, (3) if the number can be reached, a VoIP call is initiated, and (4) if the number cannot be reached over the Internet, the call is routed to the traditional telephone network.

ENUM-compliant technologies and implementations are still in the development and testing stages. A number of nations around the world have initiated formal ENUM "test bed" implementations. The United States Department of Commerce has endorsed the U.S.'s participation in ENUM, and set out a series of guidelines to be met before formal tests or government-sanctioned implementations can proceed. Commercial deployment of ENUM services is likely to take place by the end of 2004.

---

(3) Policy Issues Raised by ENUM ENUM's potential benefits also bring risks in terms of privacy and other public policy concerns. The simplest implementation of ENUM envisions that individuals' personal contact information (such as telephone numbers and e-mail addresses) will be stored in special records located in the Domain Name System (or DNS) of the global Internet. Because the DNS is publicly available, ENUM could significantly compromise the privacy of its users, and could lead to additional spam and other problems.

A more complex use of ENUM (in conjunction with a device called a "proxy server"), however, offers the opportunity to gain the benefits of ENUM without sacrificing control over personal information. To minimize the potential harmful effect of ENUM on privacy, it is vital that this second, more complex approach to ENUM be permitted and available in the marketplace.

Other important issues turn, for example, on (a) how much information individuals or companies will be required to provide in order to take advantage of ENUM, and (b) how much of that information will be revealed in a public database (similar to the "whois" database which reveals information about domain name holders).

In a different vein, ENUM raises a range of policy issues about how closely "ENUM numbers" should be tied to existing traditional telephone numbers.

One critical aspect of the global public policy issues surrounding ENUM is the fact that ENUM will, for the most part, be implemented within each country by the telephone authorities or companies that operate within that country. Thus, many critical decisions (for example, about how much information will be required to obtain an ENUM number) will be made on a country-by-country basis. It is critical that within each country, the relevant telephone authorities must closely consult with the public interest and civil society sector, the communications industry, and the computer industry.

---

(4) Recommendations for ENUM Implementations To ensure that users can take advantage of ENUM without sacrificing privacy, any implementation of ENUM should follow a number of guidelines to ensure that there is a diversity of ENUM service providers and that those providers will be able to offer privacy-protecting ENUM options. CDT's report on ENUM details 14 specific policy recommendations. Among the specific recommendations are:

- At no time should *any* ENUM record be created without the express consent of the individual or entity that subscribes to the corresponding telephone number on the traditional telephone network. An ENUM user should explicitly "opt-in" to the ENUM service.
- No publicly accessible whois-like database of ENUM subscribers should be created.
- Prospective ENUM users should receive clear notice of the privacy risks and consequences of using ENUM.
- ENUM policy within a country should be set in close consultation with the public interest and civil society sector, the communications industry, and the Internet industry.

CDT's report on ENUM also provides a bibliography of references and links to ENUM resources and analyses.

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

CDT POLICY POST
Volume 9, Number 10, May 13, 2003

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

(1) Authentication Privacy Principles Working Group Releases Interim Report "Authentication" can be a buzzword meaning different things to different people. "Identity authentication" systems are intended to make it easier to authenticate individuals online and facilitate the sharing of personal information. These systems are being developed to address problems ranging from consumer convenience to identity theft to homeland security. While identity authentication may indeed help solve vexing online problems, it also raises numerous, unresolved issues of privacy, security and governance.

Privacy is especially important. Privacy is a crucial component of trust, and without user trust, the new systems will simply not find a market or public acceptance. Many of the key players creating authentication tools understand the importance of trust and have embraced the idea of building privacy into authentication technologies.

Over the past seven months, CDT, several other consumer groups, and privacy experts have engaged in a dialogue with many of the leading vendors of authentication technologies to develop a consensus set of privacy principles to guide the development of authentication systems for consumer-initiated transactions and government services.

Tomorrow, May 14, at the Federal Trade Commission's workshop on "Technologies for Protecting Personal Information: The Consumer Experience," the Authentication Privacy Principles Working Group convened by CDT will release an Interim Report setting forth six consensus principles for the development, procurement and use of authentication technologies.

(2) Key Elements of the Authentication Privacy Principles The Privacy Principles being released by the Working Group state that authentication systems for consumer-initiated transactions and government services should:

1. Provide User Control - The informed consent of the individual should be obtained before information is used for enrollment, authentication and any subsequent uses.
2. Support a Diversity of Services - Individuals should have a choice of authentication tools and providers in the marketplace. While convenient authentication mechanisms should be available, privacy is put at risk if individuals are forced to use one single identifier for various purposes.
3. Use Individual Authentication Only When Appropriate - Authentication systems should be designed to authenticate individuals by use of identity only when such information is needed to complete the transaction. Individual identity need not and should not be a part of all forms of authentication.
4. Provide Notice - Individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions.
5. Minimize Collection and Storage - Institutions deploying or using authentication systems should collect only the information necessary to complete the intended authentication function.
6. Provide Accountability - Authentication providers should be able to verify that they are complying with applicable privacy practices.

The full Interim Report of the Working Group including details about these principles can be found at http://www.cdt.org/privacy/authentication/030513interim.pdf and http://www.cdt.org/privacy/authentication/030513interim.shtml

The following companies and organizations participated in the Working Group's efforts to develop the Authentication Privacy Principles and are encouraging their consideration in the development, procurement and use of authentication technologies: Center for Democracy and Technology; Consumer Action; Corporate Privacy Group; eBay; Hewlett-Packard; Intel; Liberty Alliance; Microsoft; NeuStar; TRUSTe; and VeriSign.

---

(3) Background on Authentication and Privacy New technologies for authentication have the potential to make online transactions more seamless, tie together information on multiple devices, enable new services, and take us closer to a pervasive computing society. However, many authentication systems will collect and share personally-identifiable information, creating privacy and security risks. To mitigate these risks, it is essential that authentication systems be designed to support effective privacy practices and offer individuals greater control over their personal information.

The release of Microsoft XP and its expanded use of the Passport authentication system, along with the release of the Liberty Alliance 2.0 specification, have intensified the focus on authentication technologies and the questions they raise about privacy and security.

In the Summer of 2001, a number of privacy and consumer groups filed a complaint at the Federal Trade Commission (FTC) challenging Microsoft's marketing and use of the Passport technology. The complaint led to a consent agreement between the Commission and Microsoft, under which Microsoft agreed to build a privacy and security program for Passport to be monitored by the FTC.

The Microsoft/FTC Consent Agreement can be found at -- http://www.ftc.gov/os/2002/08/microsoftana.htm

The European Union Working Group on Data Protection also came to an agreement with Microsoft to make changes to Passport to help protect the privacy of users. The agreement included a report about the privacy implications of Passport and online authentication generally.

The EU report can be found at --
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf

A group of companies called the Liberty Alliance has designed its own standard for digital authentication and information exchange. This group released the 2.0 version of its specification in April. It includes rules for the sharing of attribute information, including a basic language for information about individuals. While the specification itself has few privacy or security rules, the Liberty Alliance also released a detailed set of privacy and security guidelines, which are consistent with the Authentication Privacy Principles being released by the Working Group.

The Liberty Alliance Privacy and Security Guidelines can be found at --
http://www.projectliberty.org/specs/draft-lib-arch-security-privacy-v1.0-05.pdf

Another area of privacy concern is the development of authentication systems for e-government services. Many e-government projects intend to develop and or utilize authentication systems. However, this raises not only concerns about the use of personal information similar to those arising in the commercial context but also concerns about the creation of a centralized government identity system or card.

The National Research Council recently released an excellent report on privacy and authentication. This report, entitled "Who Goes There? Authentication Through the Lens of Privacy," is available at http://www7.nationalacademies.org/cstb/pub_authentication.html

While a main focus of many authentication technologies has been their use on the Internet, these same technologies can be employed offline, utilizing smart cards and/or biometric identifiers (such as fingerprints or iris scans) to help identify individuals in the real world. Therefore, the NRC report and the Authentication Privacy Principles being issued by the Working Group focus on authentication both online and offline.

---

(4) Future Work of the Authentication Privacy Principles Working Group The Authentication Privacy Principles are intended to serve as guidance for companies now developing authentication systems. The goal is to encourage developers to build privacy and security protections into authentication technologies to use in consumer-initiated transactions and government services. The principles will also serve as a marketplace guide for individuals and companies deciding which authentication system to implement or adopt.

In the coming months, the Working Group will develop its final report, expected to be a more detailed document that will explain how the Privacy Principles would work in day-to-day transactions. Separate sections will describe how the principles apply to the two areas of consumer-initiated transactions and government services, with explanatory scenarios. The Working Group is not considering the separate question of authorization and security applications that may utilize credentials created in the authentication process. Also in a separate effort, CDT is creating a working group to develop privacy guidance for the related but distinct questions that arise from the sharing and use of personal information for data mining or pattern analysis.

The Working Group appreciates input and support from all interested parties in its ongoing process. Organizations, companies and individuals interested in learning more about the Authentication Privacy Principles or the Working Group process can email appwginterest@cdt.org.

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

CENTER FOR
DEMOCRACY
&
TECHNOLOGY

CDT POLICY POST
Volume 9, Number 11, May 19, 2003

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

(1) Peer-to-peer Users Should Beware of Privacy and Security Issues In testimony before the House Government Reform Committee May 15, CDT Associate Director Alan Davidson raised concerns about the privacy and security of popular peer-to-peer (P2P) file sharing networks. P2P programs such as Kazaa, Grokster, and Morpheus are among the most downloaded computer software today. P2P file-sharing tools have become notorious for fostering widescale piracy of copyrighted works -- an activity that CDT condemns, and that carries significant legal penalties. These P2P tools can also raise potential privacy and security risks for those who share files.

CDT noted that carelessness in installing and using file-sharing software can result in the unintended sharing of users' sensitive personal information. Key privacy and security concerns facing users include:

- Inadvertent sharing of sensitive personal information;
- Spyware that communicates without a user's knowledge; and
- Legal risks both for those who violate copyright law, and due to certain overly broad subpoena powers granted under law

P2P file sharing has many legitimate uses, is largely in the control of those who use it, and is decidedly hard to regulate. CDT called for a broad public education effort and improved software practices to better inform people about the potential privacy and security risks of file sharing while preserving the benefits of this technology. CDT also called for application of fair information practices to spyware and modifications to existing law including baseline privacy legislation for the Internet.

CDT's testimony is available at http://www.cdt.org/testimony/030515davidson.pdf [PDF] and http://www.cdt.org/testimony/030515davidson.html [HTML]

---

(2) Risks From Inadvertent Sharing Of Sensitive Files Peer-to-peer file sharing systems provide Internet users with the ability to share files on their computers with thousands or millions of other people. In doing so they make it possible, and in some cases too easy, for people to share even very personal files, sometimes by accident.

Recent studies have found dozens of examples of Kazaa users who have made available for download sensitive documents on their computers like their tax returns, e-mail inboxes, or check registers -- almost certainly by mistake. Once available, these sensitive files could be used to commit fraud, invade privacy, or even commit identity theft.

In many respects this issue is akin to the problems facing any speaker on the Internet, who might mistakenly share sensitive files. But several factors heighten the privacy concern for file sharing systems. These networks are used by millions of consumers, typically with far less expertise than publishers on the Web. P2P networks' powerful search capabilities can make files more widely accessible than other publishing tools. And in many cases finding out just what is being shared is not that easy, especially for those unfamiliar with the workings of these programs.

Though the consequences of mistakenly sharing personal files are sobering, it is important to keep the problem in perspective. Reports by the General Accounting Office and the Federal Trade Commission indicate that Internet sources of information constitute a very small percentage of identity theft cases, and available data seems to indicate that the percentage of peer-to-peer users who inadvertently share sensitive files is small.

CDT believes that education is the key to helping users protect themselves from the dangers of over-sharing on P2P file networks. Resources such as GetNetWise.org offer guides to safe use of these systems. Also, the developers of P2P software can and should make it easier for users to understand and control what they share.

Information about safe file-sharing online is available at: http://security.getnetwise.org/tips/filesharing/

---

(3) "Spyware" Violates Privacy, Denies User Choice Many file-sharing programs contain "spyware" that collects information about a user's online activities, then communicates that information back to a third party, typically without the user's knowledge or consent. While often used primarily for sending ads, spyware can be used for more invasive collection of information. These programs can be difficult for users to detect or even remove, and may seriously affect the stability and security of a user's computer.

CDT strongly believes that developers of file-sharing software, like any developer that includes spyware, should observe fair information practices. They should give users clear notice about the type of information being collected about them, meaningful choices about whether to participate, and access to personal information being collected and retained.

In their current form, many file-sharing applications fail to meet these fair information practices. Notice about the installation of these programs is often buried in complex click-through agreements. The ability to opt-out of data collection often does not exist, even through the use of third-party spyware blocking systems.

CDT urges consumer to avoid applications with spyware and demand best practices for the handling of their personal information.

More information about Fair Information Practices is available at
http://www.cdt.org/privacy/guide/basic/fips.html

(4) Other Legal Risks In Peer-to-peer Networks File traders who violate copyright laws face obvious legal risks. CDT condemns the piracy of copyrighted works. Those who engage in it face substantial legal penalties.

At the same time, CDT is concerned that at least one provision of current law -- the broad subpoena power granted to any copyright holder under Section 512(h) of the Digital Millennium Copyright Act (DMCA) -- too easily allows the identity of peer-to-peer participants or any Internet user to be unmasked wrongly or by mistake without their knowledge.

As recently interpreted in a federal court decision in RIAA v. Verizon, this DMCA subpoena authority would permit any copyright holder -- possibly millions of people and groups -- to compel an ISP to disclose the identity of an Internet user based on an allegation of copyright infringement. This disclosure of personal information would take place without requiring any notice to the user that his or her identity had been unmasked, and without much judicial oversight as to the likely truth of the allegations. Accepting the importance of fighting massive copyright infringement online, we are concerned that personal data about users will be revealed inappropriately due to misuse, abuse, or mistakes.

Effective copyright enforcement need not come at the expense of individual privacy. For example, providing end users with notice when their identity is revealed would go a long way toward preventing abuse and could even enhance enforcement by warning users about potential infringing activity. Courts could be required to exercise greater oversight. Sanctions could be put in place for misuse. Reporting requirements could be established to ensure that provisions were not being misused. CDT believes that a better privacy balance can and should be struck by Congress.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

CDT POLICY POST
Volume 9, Number 12, June 23, 2003

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

(1) Supreme Court Finds Library Filtering Law to be Constitutional In a fractured decision today, the U.S. Supreme Court upheld as constitutional a law that requires federally-funded public libraries to filter Internet access. CDT continues to believe that the federal law -- known as the Children's Internet Protection Act, or CIPA -- is unwise and unnecessary. The decision upholds a Congressionally-mandated, one-size-fits-all solution to a problem that is far better addressed at the local level. Local communities, and their professional librarians, are better equipped than Congress or the courts to determine how best to protect children online.

None of the five opinions in the case garnered the support of a majority of the Court, but five of the nine Justices did make it clear that it would be unconstitutional if libraries used filtering software to prevent adults from accessing lawful content over the Internet. In essence, this means that librarians must turn off or disable the software in response to requests from adults.

Today's decision highlights the critical need to improve content filtering software, which today blocks access to lawful and valuable speech. Libraries can and should take the lead in demanding that filtering software be much more "First Amendment friendly."

The decision of the U.S. Supreme Court can be found at http://www.cdt.org/speech/cipa/030623decision.pdf

(2) Law Links Federal Library Funds, Filtering The Children's Internet Protection Act (CIPA) was passed by Congress in 2000. After courts ruled unconstitutional two previous attempts at regulating online publishers -- the Communications Decency Act (passed in 1996) and the Children's Online Protection Act (passed in 1998) -- CIPA sought to limit access to certain kinds of Internet content by users in public libraries and schools.

A large percentage of libraries and schools receive federal support to help defray the ongoing costs of providing Internet access and other services. CIPA would cut off that funding for any library or school that does not install and use Internet filtering software on all Internet-enabled computers. CIPA requires that these filters be equipped to block access to child pornography, obscenity, and material that is "harmful to minors." The statute states that adults wishing to access material that is lawful but blocked by the filters would be able to request access to the blocked sites.

The American Library Association, the American Civil Liberties Union, and others challenged the law after its passage, and the U.S. District Court for the Eastern District of Pennsylvania blocked its enforcement in 2002. Today's Supreme Court decision reversed that lower court injunction.

CDT opposed CIPA's passage and filed a friend-of-the-court brief in the Supreme Court supporting the lower court's decision to enjoin CIPA's enforcement. CDT believes that, while filters are imperfect tools, they can help keep offensive material away from children when used voluntarily by families. Federally mandated use of those filters, however, denies adults access to material they are entitled to view under the First Amendment. In addition, when required by government, filtering imposes a "one-size-fits-all" approach to managing online content that denies the diversity of American communities. It forces communities to endure the downside of filters -- namely, their tendency to overblock constitutionally-protected material -- without considering other options that might better serve their interests.

For more background on CIPA and the litigation, go to http://www.cdt.org/speech/cipa/

---

(3) Libraries Must Demand Better Filtering Software The CIPA decision highlights the critical need to improve content filtering software, which today blocks access to lawful and valuable speech. CDT calls upon the library community to use filters wisely and to insist that they foster free speech values. Filters can be more First Amendment-friendly if they make clear what sites are blocked, and if they can be customized to suit the needs of local communities.

The Supreme Court decision today does not mean that all libraries in America must install highly restrictive filters. Libraries that do not accept certain federal funds need not adopt filtering at all, and CDT urges them to adopt a policy most appropriate to their communities. Moreover, even covered libraries can pick and choose among available filtering software, which varies widely.

Librarians are well-situated to understand the public's need for access to a broad range of content, and those librarians must demand improvements in filtering software. Librarians should play a larger role in ensuring that filters do not block valuable content, and that filters are more transparent about what is and is not blocked.

---

(4) Taken Together, Justices' Opinions Uphold Adults' Right of Access Chief Justice Rehnquist wrote the "plurality" opinion, on behalf of himself and Justices O'Connor, Scalia, and Thomas. Justices Kennedy and Breyer both filed separate opinions agreeing that CIPA should be upheld, but emphasizing very different considerations. Justices Stevens, Souter and Ginsberg would have struck CIPA down, and they wrote or joined dissenting opinions.

The two concurring opinions of Justices Kennedy and Breyer are critical. Those opinions plus the views of the three dissenters make clear that that filtering software cannot be used to block adults' access to lawful content on the Internet. As Justice Kennedy made clear in his opinion, the law might well be unconstitutional if adults are not easily able to get access to lawful content on the Internet.

Justice Kennedy's opinion on adult access is largely based on an oral argument exchange that he had with Solicitor General Ted Olson, who argued for the government. Kennedy asked a series of questions probing what a library patron must do to get the filtering removed. Olson told the Supreme Court that a patron does not need to give any explanation as to why he wants the filter disabled. He also suggested that a patron can ask that filtering be entirely disabled without specifying individual web sites to be unblocked.

The concurring Justices seem to have written those two points into their interpretation of the law. Here's what Justice Kennedy said, "If, on the request of an adult user, a librarian will unblock filtered material or disable the Internet software filter without significant delay, there is little to this case. The Government [i.e., Mr. Olson] represents this is indeed the fact."

A transcript of the oral argument is available at
http://www.supremecourtus.gov/oral_arguments/argument_transcripts/02-361.pdf

---

(5) Education and Enforcement Are the Best Paths to Online Safety Notwithstanding the Court's decision today, several studies, including the Report of the Commission on Children's Online Protection Act and the National Research Council report, "Youth, Pornography and the Internet," have concluded that legislation simply will not work to protect children from inappropriate material online. CDT believes that giving users control over what they see and do online -- through education and through tools such as those collected at sites like http://www.getnetwise.org -- will more effectively protect kids in ways consistent with their own family values, and consistent with the Constitution.

The government's appropriate role should be to encourage and foster education for children and families about how to assure a safe, positive online experience. It should, in addition, devote increased resources to better enforcement of laws against child pornography and child sexual exploitation.

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

The report of the COPA Commission is available at http://www.copacommission.org/report/.

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