CDT POLICY POST Volume 10, Number 1, January 22, 2004

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

---

(1) CDT Launches Election 2004 Youth Political Empowerment Project

Last Fall, CDT launched Youth04, a project that seeks to synthesize the best of the political Internet with the best of traditional grassroots organizing to empower and motivate 18-25 year olds in the 2004 elections. The project is headed by CDT senior policy fellow David M. Anderson, founder of Maryland Internet Politics Week and an adjunct professor at George Washington University's Graduate School of Political Management.

Much of the leadership and momentum of Youth04 comes from College Chapter Leaders that Youth04 is recruiting and training. Sixteen chapters are currently underway, including at the University of Washington, Harvard, the University of South Carolina, Clemson, Howard, George Washington University, and the University of Texas.

Youth04 has forged partnerships with major organizations focused on young voters, including: Youth in Action, Mobilizing America's Youth, United Leaders, Party Y, and Youth Venture. Other Youth04 partners

providing content and outreach include Harvard's Institute of Politics, the University of Washington's Center for Communication and Civic Engagement, George Washington University's Graduate School of Political Management, The Junior State of America, The Washington Center, and People for the American Way.

In an op-ed last year in the Baltimore Sun, Youth04 head David Anderson outlined the philosophy behind Youth04: "Next step for Net: engaging undecided voters."

The Youth04 website is at http://www.youth04.org.

---

(2) W.W. Norton Releases Youth04 Online Student Guide

On January 15, W.W. Norton & Company released an online version of "Youth04: Young Voters, the Internet and Political Power." This booklet, written by Youth04 Executive Director David Anderson, sets forth both a theoretical and practical guide to college students who wish to become empowered this election year. Norton will market this booklet in hard copy in the Fall in conjunction with the most widely used political science textbook in America, "We the People," by Benjamin Ginsberg, Theodore Lowi, and Margaret Weir.

The Youth04 website also contains a College Curriculum page with useful links and suggested topics for papers and discussions, designed to help college professors raise in their classes questions about young voter engagement.

"Youth04: Young Voters, the Internet and Political Power" is online at http://www.wwnorton.com/wtp4e.

---

(3) Youth04 Seeks to Create Relationship between Candidates and Young Citizens

Youth04 is focused on giving young voters a voice in the 2004 elections, in races from President on down. To bring the beliefs and

sentiments of young voters to the candidates, online and offline strategies will be employed, including Web-based efforts like petitions and online votes that will aggregate the viewpoints of young voters. Two Youth04 discussion boards are up, with more to follow. Candidates are being urged to make postings.

The project also intends to use viral political marketing techniques. A petition that seeks to affirm young voters' desire to become empowered this election cycle is currently circulating around the Net.

Youth04 is encouraging restaurants and cafes to provide discounts to young people who wish to meet to discuss politics. Youth04 Chapters is also seeking to forge relationships with nonstudent 18-25 year olds at community technology centers in an effort to bridge the civic divide, which lines up in many ways with the digital divide.

---

(4) Youth04 Targets South Carolina for First Primary Effort

Youth04 has launched it first targeted effort in South Carolina. With two weeks to go before the pivotal February 3 primary, Youth04 has three college chapters (USC, Clemson, and Claflin,an historically black college) working to create a relationship between young voters and the candidates.

South Carolina Youth04 has its own webpage, which now features a contest between USC and Clemson, arch rivals, to generate the most signatures on a petition urging politicians pay attention to young people.

In the primary season, Youth04 is also targeting Wisconsin, Massachusetts, Maryland, and Ohio for special attention.

The South Carolina Youth04 webpage is http://www.youth04/states/sc/

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

CDT POLICY POST
Volume 10, Number 2, January 26, 2004

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

---

(1) Supreme Court to Consider Net Content Controls; CDT Files BriefCDT is urging the Supreme Court to rule unconstitutional a federal law that would place limits on legal Internet speech. Joined by a broad coalition of organizations representing Internet companies, publishers and others, CDT filed on January 15 a "friend-of-the-court" brief challenging the Child Online Protection Act (COPA).

COPA, adopted in 1998 but blocked from taking effect by lower courts, would make 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 used technological means to prevent access by minors (such as requiring a credit card). COPA would impose criminal and civil penalties of up to $50,000 per day for violations. "Harmful to minors" is a legal category that includes a wide range of social commentary and health information that is legal for adults to view.

The range of organizations signing the brief reflects the broad concern with COPA's implications for the Internet and free expression. Those signing the brief included high-tech trade associations such as the Information Technology Association of America and the Computer and Communications Industry Association, content industry groups such as the Association of American Publishers and the Recording Industry Association of America, news media organizations such as the Newspaper Association of America and the Society for Professional Journalists, and the Freedom to Read Foundation of the American Library Association, a longtime advocate of the Internet as a medium for free expression and access to information.

The case is Ashcroft v. ACLU. Oral argument is scheduled for March 2, 2004. The Court's decision is likely to be issued in late May or June of this year.

The coalition brief is at http://www.cdt.org/speech/copa/20040115amicus.pdf.

---

(2) COPA, However Well Intentioned, Restricts Legal Speech OnlineCOPA is another Congressional law passed in the name of protecting children that would "burn the house to roast the pig," to quote the Supreme Court's landmark 1997 decision on Internet free speech. The CDT brief argues that:

- COPA imposes serious burdens on constitutionally-protected speech.
- COPA fails to effectively serve the government's interest in protecting children, as it will not prevent children from seeing inappropriate material originating from outside of the US or material available through other Internet resources besides the World Wide Web, such as chat rooms or email.
- COPA does not represent the least restrictive means of regulating speech.

This is COPA's second trip to the Supreme Court. In May 2002, the Supreme Court found fault with the reasoning of a Court of Appeals that had ruled the law unconstitutional, but the Supreme Court left in place an injunction against the law.

On reconsideration, in March 2003, the appellate court again ruled against the law, finding numerous constitutional problems with it. In a detailed decision, the appeals court determined that COPA would force Web publishers to block a wide range of legal material and was not the least restrictive means of protecting children online. The Justice Department appealed, bringing the case back to the Supreme Court.

More on COPA: http://www.cdt.org/speech/copa/

---

(3) Education and User Control, Not Legislation, Key to Protecting Children Throughout the course of the challenge to COPA, CDT has argued that the most effective way to protect children online, and the means least restrictive of free expression, is by putting resources at the disposal of families and teachers that allow them to control what children see and do online. This approach enables the protection of children while respecting the diverse sensibilities of American families. CDT has worked with a wide cross-section of the Internet and public interest communities to compile parental tips, filtering tools and other online safety resources at the educational site http://www.getnetwise.org.

This emphasis on education and user control was confirmed by two major, independent studies commissioned by Congress: the COPA Commission, a study mandated by the COPA law itself, and a report of the National Research Council (NRC) of the National Academy of Sciences. Both studies concluded after exhaustive research that legislation will not solve the problem of children's access to objectionable content via the Internet, but rather that technologies like filtering software in the hands of parents and teachers and educational efforts offer the most effective means of protecting children online.

The NRC study, "Youth Pornography, and the Internet" (2002), is online at http://www.nap.edu/books/0309082749/html.

The 2000 report of the COPA Commission can be found at http://www.copacommission.org/report/

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

CDT POLICY POST
Volume 10, Number 3, February 3, 2004

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

---

(1) Security Holes at DMVs Feed ID Theft, Offer Lessons for National ID Card DebateCDT has released a report pointing to security problems nationwide in the issuance of driver's licenses, at a time when the card is being increasingly looked to as a general form of identification. Culling news reports in the last year alone, the report found two dozen cases in 15 states where bribery or lax security at Department of Motor Vehicle (DMV) offices had resulted in fraudulent issuance of thousands of driver's licenses. The survey offers a warning to those who think that adding more biometric information to driver's licenses will make them reliable as a de facto national ID card.

Based on the findings of the survey, CDT recommends:

- An "Accountability Index" - Congress should direct the General Accounting Office (GAO) to develop a fraud and security index for state DMV offices, ranking the states on both internal and external security, and measuring performance over time.

- Federal penalties for DMV corruption - Congress should adopt legislation to clearly make it a federal crime for a state DMV employee to accept a bribe to issue a driver's license. Federal jurisdiction is justified because the crime affects security nationwide. A federal statute would allow a federal law enforcement response where states fail to act.

- Pilot Programs for Security - Congress should offer pilot grants for new technologies, programs and training aimed specifically at rooting out fraud and improving physical security at state motor vehicle offices.

Even with these measures, CDT recommends against reliance on any system that links state driver's license data for ID purposes unrelated to highway safety. Instead, security measures should rely on the concept of multiple forms of identification for different purposes. It is a well-known, but often forgotten, principle of security that broad reliance on a single form of identification creates a single point of failure. The security breaches that CDT's report catalogues in DMV offices across the country are a reflection of the incentives for fraud already being generated by overburdening the driver's license as a general purpose ID card.

CDT's report, "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses," is at http://www.cdt.org/privacy/20040200dmv.pdf.

---

2) Driver's License Facing Wider Uses, including Online Authentication The state-issued driver's license is playing an important role in an increasing range of areas:

- Highway safety - Public safety depends on the ability of authorities to properly issue and revoke driver's licenses.
- Identity fraud and theft - As merchants use the driver's license as an identifier, the licenses have become a tool frequently used to perpetrate identity fraud. Identity theft is regularly cited as the fastest growing crime in America.
- Homeland security - Since September 11, 2001, heightened attention has been given to the driver's license issuance system in the United States. Several of the 9/11 hijackers had driver's licenses illegally obtained through state motor vehicle offices. The hijackers' use of these as their ID cards at the airports illustrated all too well that the driver's license has become more than just a license to drive.
- Online authentication - Proposals to create "smart" driver's licenses that could be used with a card reader on a computer for online authentication have far-reaching implications, which drew CDT into this area in the first place. Individuals and e-commerce sites cannot use traditional face-to-face techniques to establish identity, posing some difficult issues around trust online. Some companies and policymakers searching for stable online credentials have proposed using the driver's license as a medium for verifying identity in cyberspace.

In 2002, several proposals were put forth to create a National ID card or, more subtly, to create a back end database connecting driver's license information across the country and to begin to incorporate digital biometric information, such as a fingerprint, into the card and the linked databases. None of the major legislation on the subject has been reintroduced in this Congress, but more moderate proposals may be introduced this session.

For more background information on the use of the driver's license as a general ID card, see:

- CDT's Policy Post 8.17: PRIVACY AND SECURITY RISKS IN DRIVER'S LICENSE PROPOSALS (Sept. 5, 2002) http://www.cdt.org/publications/pp_8.17.shtml
- The National Academy of Sciences report, "IDs -- Not that Easy" (2002) http://www.nap.edu/html/id_questions/
- "Reliable Identification for Homeland Protection and Collateral Gains" - Appendix A to the report of the

Markle Foundation Task Force on National Security in the Information Age (Dec. 2003) http://www.markletaskforce.org/.

---

(3) Lax Security and Insider Abuse at the Local Level Pose National ChallengesCDT has been concerned that policymakers interested in ID issues are too focused on the quality of the driver's license as an identity document - thus proposals to improve the biometrics on the card - and are overlooking the bigger concern that the driver's license system is riddled with fraud at the point of issuance. All the biometrics in the world won't make a secure card if DMV employees can be bribed or the card-making equipment can easily be stolen. Our concern has been that the fraud issue, of grave national consequence, was being treated mostly as a local concern.

In October 2002, CDT called upon the American Association of Motor Vehicle Administrators (AAMVA) to begin compiling an index of cases of internal and external fraud relating to the issuance of driver's licenses at the DMVs. CDT believed fraud was more widespread than realized and that all state agencies should be evaluated and ranked based on performance. When AAMVA did not take up the idea, CDT undertook a survey of local news coverage in 2003 and found:

- 23 cases of publicly reported fraud or lax security at driver's license operations in 15 different states.
- Thousands of fraudulent driver's licenses issued by bribed state employees.
- Dozens, if not hundreds, of cases of identity theft tied back to internal fraud and bad security practices.

Some of the more egregious cases include:

- The entire 11 person staff of the Newark, New Jersey DMV office was fired after investigators determined fraud was rampant. New Jersey had multiple cases of fraud or theft. This is not to suggest that NJ has the worst problem, but may just be a reflection of the fact that New Jersey has an ongoing investigation based on the consistent concerns about the state agency.
- An identity theft ring in Oregon was found with a CD-ROM full of Oregon drivers' personal information and the casings and cards that could only have been taken from an Oregon Motor Vehicles Office. Officials say that they could link at least 40 cases of identity theft back to the thieves.
- Indiana officials are still investigating a bribery ring that led to the fraudulent issuance of more than 1000 licenses across the state.

CDT POLICY POST
Volume 10, Number 4, February 19, 2004

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

---

(1) CDT Urges FCC to Protect Internet In Defining DTV Broadcast FlagCDT submitted comments to the Federal Communications Commission on January 13 in the latest round of proceedings regarding the copy-protection of digital TV (DTV) broadcasts via a mechanism called the "broadcast flag." The FCC has mandated that, starting in July 2005, all equipment capable of receiving DTV broadcasts must include federally approved content protection technologies. The FCC is now addressing a range of critical questions surrounding the implementation of the flag scheme. These issues include the procedure for approving protection technologies and questions about how to make the requirements of the rules compatible with increasingly popular software-based DTV applications and networkable consumer electronics devices.

CDT is working to find pragmatic solutions that balance the interests of Internet users with the intellectual property rights of content creators. Given the importance of the Internet to democratic values, CDT urged the Commission to make sure the flag rule did not "leave out the Internet" or overly burden the free flow of information online. CDT urged the Commission to ensure that users are able to make reasonable uses of content and exchange material over the Internet, so long as they do not engage in massive copying.

Specifically, CDT called on the FCC to adopt objective functional criteria for approving copy protection technologies and to develop a transparent and publicly accountable process for applying those criteria based on the narrow goal that the Commission has articulated for the flag regulations -- preventing "indiscriminate redistribution" of copyrighted content online. CDT also urged that the Commission make clear that the rulemaking is not a precedent for the FCC to take a broader role in the regulation of consumer technologies.

- CDT's comments on the broadcast flag are athttp://www.cdt.org/copyright/20040213flagcomments.pdf

- CDT's "Public Interest Primer" on the Broadcast Flag is at http://www.cdt.org/copyright/031216broadcastflag.pdf

- The FCC's broadcast flag ruling is athttp://www.cdt.org/copyright/031104fcc.pdf

---

2) CDT Comments Focus on Potential Impacts of the Flag Rule on the Internet and Innovation Online
The broadcast flag regulations represent a specific response to some of the considerable challenges posed for copyright holders by the increasing importance of computers and networks in emerging digital media. However, these technologies also hold tremendous potential to foster expression and civic discourse, and CDT argued that the Commission must be wary of imposing undue burdens on their development and use.

While the FCC indicated in its earlier ruling that it intended for the flag regulations to "facilitate innovative consumer uses and practices, including use of the Internet as a secure means of transmission," (FCC Report and Order, November 4, 2003) some commenters suggested tightening the flag rule in ways that would severely limit the uses consumers can make of digital broadcast content online.

CDT and others argued, instead, for an implementation of the rule that focuses on the Commission's narrow expressed goal of frustrating mass, "indiscriminate redistribution" online, without obstructing secure private transmission over the Internet or other uses of broadcast content on personal computers and digital networks. Other groups that argued for a similar, narrowly tailored, implementation of the flag regulations include the Business Software Alliance, the Computer Systems Policy Project, Verizon, Phillips Electronics, and consumer groups Public Knowledge and Consumer's Union.

---

(3) CDT Argues for Narrow, Objective Approval Process for New Technologies, with Regular OversightCDT said in its comments that continued innovation and free expression on the Internet is best protected by the development of a robust marketplace in content protection technologies. Such a marketplace ensures that consumers have real choices among rights protection options and that developers have strong incentives to find ways to meet consumer demands for reasonable and innovative uses of content while maintaining appropriate protections for copyrighted works.

CDT suggested several specific measures to ensure that the Commission's approval process for new technologies does not create unnecessary barriers for technology developers:

- adopting objective functional criteria for approving technologies, based on the narrow goal of preventing indiscriminate redistribution online;

- adopting a lightweight self-certification process by which technology developers can assert that they have met these criteria;

- adopting a flexible, predictable, transparent, and publicly accountable process for rapid resolution by the Commission of challenges to such self-certifications;

- establishing an independent oversight board to periodically reexamine the flag rules' impacts on interoperability of new compliant technology with legacy devices, reasonable consumer expectations,

and consumers' ability to access information online;

- refraining from any attempt to exhaustively define the realm of permitted uses and thereby ruling out new and innovative uses that may arise.

---

4) CDT Warns Flag Should Not be Used as a Precedent for Further RegulationCDT also argued in its comments that the Commission must make it clear that the flag cannot be viewed as a precedent for broader regulation of technology. The specific rationale and processes put in place to deal with the special case of digital broadcast content protection are not sufficient to justify broad re-architecting of all digital technology. For example, CDT is concerned with the potentially sweeping ramifications of the Commission's stated intention to consider mandated protection measures for analog outputs. Most televisions, VCRs, and DVD players now in consumer's homes are connected through analog outputs and inputs. To be effective, a technological protection measure for these analog signals would require broad regulation of devices containing analog-to-digital converters, including personal computers and many consumer electronics devices.

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

CDT POLICY POST
Volume 10, Number 5, February 26, 2004

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

---

(1) GAO Echoes CDT Criticisms of CAPPS II; Coalition Calls for Hearings Two recent reports -- a highly critical audit of the government's proposed airline passenger screening system and an internal review of the disclosure of JetBlue records to the Army -- and the launching of a data collection system at US entry points highlight the lack of privacy guidelines for use of personal information in efforts to prevent terrorism. Taken together, the actions demonstrate why addressing privacy is crucial to developing any effective anti-terror information sharing and analysis system.

On February 16, the General Accounting Office (GAO) issued its Congressionally-mandated report on the proposed Computer-Assisted Passenger Pre-Screening System (CAPPS II). The GAO echoed many criticisms made last year by CDT and confirmed the need for a ground-up redesign of the proposed program. According to the GAO, the Transportation Security Administration (TSA), which is responsible for airport screening, has not shown that the proposed new system would be effective in identifying possible terrorists and has not resolved key privacy and due process issues. GAO reported that the system is behind schedule and faces further delays because TSA has not developed key testing, scheduling and cost plans, nor crucial privacy oversight and passenger redress mechanisms.

The GAO report does not spell the end of efforts to develop a new passenger screening system. The current method of passenger screening, which uses static behavioral criteria and airline-operated "no-fly" lists, is widely recognized as ineffective. It also has created significant problems for passengers with names similar to those on "no-fly" lists who are delayed every time they fly. A new system is needed, but CDT believes that privacy advocates, government officials and industry representatives should go back to basics, working together to develop a system that is both effective and privacy-protective.

In response to the GAO Report, a coalition of organizations from the left and right sent a letter to key congressional committees asking for hearings on CAPPS II.

- GAO Report, Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, February 2004: http://www.gao.gov/cgi-bin/getrpt?GAO-04-385.

- Coalition letter seeking congressional hearings, February 17, 2004: http://www.cdt.org/security/usapatriot/20040217cappsii.pdf.

---

(2) DHS Privacy Office Issues Report Criticizing JetBlue Disclosure In a related story, the Department of Homeland Security's Chief Privacy Officer issued a report on February 20 critical of TSA's role in the disclosure of passenger data by JetBlue to an Army contractor. The report acknowledged that while TSA did not receive the information itself, it played a role in approving the data transfer. The Privacy Office recommended privacy training for DHS employees and further review by the DHS Inspector General, and called for guidelines to govern data sharing between the private sector and the government.

A related investigation into the Army's role in the data transfer, including potential Privacy Act violations, is being conducted by the Army Inspector General but has not yet been released.

Senate Government Affairs Committee Chairwoman Susan Collins (R-ME) and Ranking Member Joeseph Lieberman (D-CT) have also expressed concerns with the role of both the Army and TSA and have said that they will continue investigating.

- DHS Privacy Office's Report to the Public on Events Surrounding jetBlue Data Transfer, February 20, 2004: http://www.cdt.org/privacy/20040220dhsreport.pdf.
- Letter from Senators Collins and Lieberman to Under Secretary Hutchinson asking for more details about TSA's involvement, February 13, 2004: http://www.cdt.org/privacy/20040213tsaletter.pdf.
- CDT Policy Post 9.20, JetBlue Disclosure Prompts Multiple Inquiries, Underscores Need for Clearer Privacy Rules, October 17, 2003: http://www.cdt.org/publications/pp_9.20.shtml.

---

(3) Privacy Plans for US-VISIT Need Further Attention The government did a better, albeit incomplete job, of addressing privacy issues when it developed the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. The Department of Homeland Security (DHS) conducted a Privacy Impact Assessment (PIA), which DHS issued on January 6, 2004, the day that the first phase of US-VISIT became operational. The PIA was one of the first to be issued by a federal agency since the E-Gov Act of 2002 was passed requiring PIAs to be conducted whenever there are new collections of information.

While the PIA appropriately covered many of the important privacy issues raised by the US-VISIT program and contained a detailed description of how the program will function, CDT has urged DHS to issue PIAs for future increments of US-VISIT well in advance of implementation so that public comments can be taken into account before the new program components become operational. CDT also highlighted some critical privacy issues that the PIA did not satisfactorily cover -- redress, access to data, data retention policies and data quality.

- CDT's Comments on US-VISIT Privacy Impact Assessment for Increment 1, February 4, 2004:

http://www.cdt.org/security/usvisit/20040204cdt.pdf.

- US-VISIT Privacy Impact Assessment (PIA), dated December 18, 2003, released January 6, 2004: http://www.cdt.org/security/usvisit/.

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

CDT POLICY POST
Volume 10, Number 6, April 12, 2004

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

---

(1) Google's GMail Highlights General Privacy Concerns Google's proposed GMail service, announced recently, has receivedwidespread attention and attracted a good deal of privacy criticism.Two specific features of Gmail -- its searching of the content of itsusers' email in order to serve targeted ads and its offer to store onGoogle's servers enormous volumes of old email -- do raise privacyconcerns. However, Google has been quite clear about these features,giving potential users the ability to weigh the pros and cons of theservice. Moreover, it is important to note that most of the privacyconcerns associated with Gmail are the same as or similar to concernsposed by other similar services, albeit heightened because of themagnitude of what GMail is proposing.

Simply put, on the content searching issue, ISPs and other serviceproviders are already using machines to scan the contents of email,especially to block spam. As to the risks of remotely storing email,users and policymakers need to be aware that, under current statutoryand caselaw, any records stored on the server of a third party -documents, calendars, email - do not enjoy the same privacyprotection as materials stored in one's own home or on one's harddrive.

In this Policy Post, CDT offers some preliminary recommendations toGoogle and other providers of similar services. We also renew callsthat we have made over the years for legal reforms that will extendstronger privacy protection to personal materials stored withWeb-based services.

---

(2) Background on Web Email and GMail For several years, various companies have provided email service onthe Web to consumers who agree to receive ads while they are lookingat incoming mail and to allow ads to be appended to their outgoingmail.

In many ways, these services exemplify the democratizing potential ofthe commercial Internet. They are open, flexible, globallyavailable, and, in most cases, free. Individuals can set up multipleaccounts for different purposes. In the context of concerns overworkplace privacy, CDT has suggested that individuals in theU.S.utilize these free accounts instead of work email addresses whensending personal email because, under current law, an employer canmonitor email sent and received over the employer's system.

Last week, the Internet search company Google announced that it wastesting a new Web e-mail service of its own called GMail. Theservice has three features that distinguish it from other free emailservices:

- Increased Free Storage -- Other Web mail services offer 2-6 MB ofstorage for free. GMail will provide up to 500 times that amount ofstorage for free - 1GB. As with other services, the storage includesnot only email, but attachments, expanding the number of documentsthat users can store remotely.
- Searchability of Mail -- Most Web mail services allow individualsto create folders to store mail. GMail uses the Google search engineto help users find their email messages, further encouraging users tokeep large volumes of material with the assurance that the searchengine will find it for them.
- Content-Based Ads -- Most Web mail services give pop-up ads orbanner ads to individuals based on profiles that they provide at thetime of sign-up. Instead, Gmail will scan through the contents ofeach message and dynamically place ads based on the subject matter ofthe email. Google promises that only computers will see the contentof messages and that no permanent information will be attached to anymessages or tied to the user based on the scan.

---

(3) Policy Concerns Associated with Content Searching Generally speaking, all email communications in the U.S. areprotected by the Electronic Communications Privacy Act (ECPA), whichrequires a court order for government interception of email intransit or in storage incident to transmission. Generally, ECPAprohibits service providers from reading the email of their customersunless the customer has given consent. One exception, however,allows ISPs to scan the content of their customers messages in orderto "protect the rights or property" of the service provider. Foryears, under this authority, ISPs have been scanning the content ofmessages to look for spam and email infected with viruses, amongother purposes. This is legal under ECPA despite the fact that theISP may not have received the direct consent of the sender of theemail, because the service is doing so to protect its rights orproperty (i.e., its servers).

However, all ISPs should probably also be very clear in their termsof service and their privacy policies as to what they are doing toscan the contents of email. And since Google's searching of contentsgoes beyond spam detection, Google will have to get very explicitconsent from GMail users.

Google's practice raises the interesting question of whether usersneed to be concerned about machines reading their email, if no humanever sees anything. In 2000, the FBI defended its Carnivore device,placed in ISPs to search the emails of many customers looking forthose to or from a designated target, by arguing that only themachine rather than a person was looking at the emails of innocentpeople.

Regardless of whether customers will put faith in the fact that amachine rather than a person is scrutinizing their email, GMailshould be based on explicit prior consent, whereas the FBI, incarrying out interceptions, does not give notice to the person orpersons whose messages are being scanned or recorded.

Google's "evolving" privacy policy for GMail explains that the onlyinformation it will use in serving ads is the name and login,collected directly from the user, and the content of the particularemail with which a given ad will be associated. Google states thatit will not ask for demographic information upon enrollment in GMail,nor will it be compiling user profiles based on email content.According to the policy, content information will not be shared withthird parties for marketing purposes.

Google has also said that it currently plans to use the same cookiefor its web search engine, GMail and all other Google services toprovide users a single sign-on. This raises the concern thatcorrelation of data between services will be very easy if Google everdecides to move in this direction. One story quotes a Googleofficial as saying that the company may in the future want tocorrelate search engine usage with email content. Google's policiescurrently state that this correlation could only be used to helpimprove GMail, not other Google services. Many other Web servicesalso use single sign-on for multiple services, although no othershave suggested that they intend to use the contents of emails to theextent Google has. Since the cookie's only benefit to the user isthe single-sign on, users that don't want the convenience can simplyblock the cookie without other impact to service. New cookie controlsin browsers offer users even greater ability to block all cookiesfrom Google or delete the cookie regularly, although only advancedusers are likely to protect their privacy in this way.

One other area of consideration are state laws on wiretapping. Anumber of states have laws that require the approval of all partiesin a communication. It is unclear how this would apply to the kindof scanning that would occur with GMail.

- GMail's Privacy Policy
- Text of 18 USC § 2701-02 (the relevant portions of ECPA)
- Privacy groups' open letter to Google on GMail
- Reporter's Committee for the Freedom of the Press "Can We Tape?" A list of state communications confidentiality laws

---

(4) Policy Concerns Associated with Third-Party Email Storage For a number of years, CDT has raised concerns about the lowstandards under which government agents and civil litigants can getaccess to personal information stored on a third party server.

ECPA was written in 1986 before the World Wide Web even existed. Atthe time, Congress was focused on protecting the privacy ofcommunications in transit, not on the protection of stored data. DOJargued that data stored with a third party did not enjoy theprotection of the warrant clause of the Fourth Amendment. ECPAadopted a two-tiered rule: email in transit or in storage incident totransmission for 180 days or less may be obtained by the governmentonly pursuant to a search warrant issued under the probable causestandard of the Fourth Amendment. Email in storage for more than 180days loses this protection and becomes a stored record that may beobtained with a mere subpoena, issued on a very low standard,normally without any review by a judge. In neither case is the userentitled to contemporaneous notice that his email is being seized bythe government. Moreover, the DOJ argues that once an email isopened by the recipient, it loses the protection of a communicationsand becomes a mere stored record, no matter how recent it is.

Also, under current federal law, ISP customers are not entitled tonotice when email is subpoenaed in civil lawsuits. This means thatindividuals in divorce cases and other civil disputes are able tosubpoena records held by an ISP or any other third party with nonotice to the owner of the email account.

Google has also pointed out that residual copies of email may remainon its systems, even after the user has

deleted them from his or hermailbox and even after a user has terminated the account. Again,this is true of all email systems, but highlights the limitations ofECPA in the area of third party storage.

CDT has recommended a series of improvement to ECPA that would updatethe law to take into account the nature of Web-based services:

- Require a warrant based on probable cause for seizure withoutprior notice of information stored on third-party systems, and priornotice and an opportunity to object for subpoena access.
- Require notice and an opportunity to object when civil subpoenasseek personal information about Internet usage.
- Require statistical reports for access to stored email, similar tothe reports required under the wiretap law.
- Make it clear that Internet queries are content, which cannot bedisclosed without consent or a probable cause order.

For more background on the law and CDT's recommended reforms, seeExecutive Director Jim Dempsey's April 6, 2000 testimony on "The Fourth Amendment and the Internet"

---

(5) CDT's Preliminary Recommendations for GMail and Online PrivacyCDT is still examining the complex issues related to GMail. Based onour preliminary research, we offer the following recommendations:

- Google should promise in its privacy policy never to correlate thecontent of email with a user's cookie or with otherpersonally-identifiable information for any purpose.
- Google should give users an active choice as to whether they wouldlike the convenience of single sign-on for multiple services orseparate log-ins (through multiple cookies).
- Google should also agree to notify users by email of any changes toits GMail policy rather than merely posting the changes to the loginpage.
- In an age of unlimited storage, lawmakers should ensure that datastored on networks is afforded full privacy protection includingproviding enhanced protection for information on networks, probablecause for seizure without prior notice, opportunity to object forsubpoena access.
- Notice and an opportunity to object should be required when civilsubpoenas seek personal information about Internet usage.

With full notice, Internet users should be able to decide whether toaccept scanning of their email in return for free services. Consumersshould be fully aware of the implications of using a system thatscans messages as a requirement for using that system. All serviceproviders should be very explicit about their practices in scanningemails for any purpose.

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

CDT POLICY POST
Volume 10, Number 7, April 20, 2004

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

---

(1) CDT Presents Consensus List of Deceptive Spyware Scenarios at FTC WorkshopA broad coalition of high tech companies and consumer advocates hascompiled a list of unfair, deceptive or devious practices involvingsoftware downloaded from the Internet - software that takes overusers' computers and resists removal, sometimes even stealinginformation. CDT presented the list at a Federal Trade Commissionworkshop on Monday, April 19 and called on the FTC to takeenforcement action against software makers and online advertisers whoengage in the condemned practices.

The list of devious practices represented an initial consensusresponse to growing concerns about the threats to Internet users'privacy posed by an array of invasive software programs referred toas "spyware." Some studies show that the majority of Internet usershave some form of "spyware" on their computers, in most cases withouteven knowing it is there.

The Consumer Software Working Group, convened by CDT, included majorsoftware and hardware companies, leading Internet service providers,anti-spyware technology vendors, and consumer and privacy groups.In an effort to begin specifying what is "spyware," and whatdistinguishes it from acceptable online practices, the group drew upa list of examples, based on real cases, of specific practicesinvolving the use or distribution of software that Working Groupmembers agreed were clearly unfair, deceptive, or devious.

The practices the Working Group identified include:

- **Hijacking** - For example, a computer user receives an Internetadvertisement when visiting a webpage. Simply as a result of loadingthe ad, a software program wholly unrelated to the advertisement orthe visited site is downloaded onto the user's computer, with nonotice or opportunity to consent.

- **Surreptitious Surveillance** - A computer user downloads softwarecontaining a keystroke logger unrelated to any functions describedto the user. The keystroke logger records all information input onthe user's computer and sends this information on to another entity.
- **Inhibiting Termination** - A computer user downloads a softwarepackage. As initially disclosed to the user, the software containsan advertising program, which generates revenue and pay for thedevelopment of the software package. However, when the useruninstalls the software, the advertising program stays on the user'scomputer.

The Consumer Software Working Group's list of "Examples of Unfair,Deceptive or Devious Practices Involving Software" is available athttp://www.cdt.org/privacy/spyware/20040419cswg.pdf

More information on spyware: http://www.cdt.org/privacy/spyware/

FTC's Spyware Workshop Page: http://www.ftc.gov/bcp/workshops/spyware/index.htm

---

(2) Much "Spyware" Already Illegal

The Federal Trade Commission Act gives the FTC the authority to takeenforcement action against unfair and deceptive trade practices. CDTand others have said that many spyware practices clearly fall withinthis jurisdiction, but so far the FTC has brought few actionsagainst spyware makers.

In November 2003, CDT invited Internet users to tell us about theirexperiences with spyware, so we could investigate specific cases andfile complaints where appropriate. In February, based on userresponses and following a careful technical investigation, CDT fileda complaint against two companies involved in deceptive advertisingand homepage "hijacking." However, the FTC has not acted upon thecomplaint.

In presenting the devious practices list to the FTC at its April 19workshop, CDT Associate Director Ari Schwartz told the Commissionthat the Working Group's agreement on unacceptable practicesdemonstrates widespread consensus that certain current practicesinvolving software are already illegal. In a preface to its list ofspyware scenarios, the Consumer Software Working Group said it "isconcerned about a specific set of devious, deceptive or unfairpractices that adversely affect consumers online. Most of thesepractices may be illegal under current law, depending on the specificfacts of the particular case."

CDT told the Commission that better enforcement of the FTC Act andother applicable statutes such as the Computer Fraud and Abuse Actand state fraud laws could have a substantial impact on the spywareproblem. Rather than wait for new "spyware" laws, CDT again calledon the Commission to go after the egregious cases that are illegalunder current law.

Information on CDT's "Campaign Against Spyware," calling on users tosend us their spyware stories, is available athttp://www.cdt.org/action/spyware/

CDT's Complaint to the FTC in the Matter of Mail Wiper, Inc andSeismic Entertainment Productions, Inc. is available athttp://www.cdt.org/privacy/20040210cdt.pdf

---

(3) Working Group Efforts Highlight Difficulty in Defining Spyware In General Terms

Several bills have been introduced in Congress to address spyware,and Utah has already adopted a law, but the Working Group'sdiscussions highlighted the difficulties in constructing a completeand precise definition of spyware and other forms of invasivesoftware without sweeping in benign practices that are standard amongsoftware companies and ISPs.

CDT has warned that, given the definitional difficulties, legislatingagainst spyware would likely prohibit ordinary, acceptable behaviorof companies that serve consumers. The Working Group echoed thisconcern, specifically noting that "the wide range of and lack ofclarity in attempted definitions for the types of software practicesthat most concern consumers hamper attempts at self-regulatory,technological and legislative responses. Many definitions of spywarein circulation today are either under-inclusive in important respectsor, more commonly, overbroad so that they include practices thatclearly benefit consumers, or both."

Rather than legislation aimed at spyware, CDT believes that theissues of privacy and user control can be better addressed by onlineprivacy legislation that would focus on the underlying problematicbehaviors rather than on specific technologies.

On March 23, CDT President Jerry Berman testified on the proposed"SPYBLOCK Act," introduced by in the U.S. Senate by Conrad Burns(R-MT) and Ron Wyden (D-OR):
http://www.cdt.org/testimony/20040323berman.shtml

---

(4) Multifaceted Approach Needed to Address Spyware Problem

In its presentation to the FTC, CDT stressed that, in the end,a combination of solutions is needed to fully address the spywareissue. Needed steps include both better consumer awareness andimproved anti-spyware technologies to give users greater control overthe software on their computers. Although the definitional issuesmake new legislation difficult, it may in the long run be necessaryas well, especially as we learn more about the problem. In the shortterm, however, stepped up enforcement by the FTC under existing lawmay have the greatest impact.

CDT urges consumers that have been affected by spyware to send theirexperiences to our campaign against spyware and to the FTC. Directfeedback from Internet users about the specific harms they havesuffered is crucial to spur a greater response from the Commission tothe spyware problem.

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

CDT POLICY POST
Volume 10, Number 8, April 28, 2004

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

---

(1) Industry and Public Interest Groups Oppose FBI Attempt to Extend Wiretap Design to the Internet
On April 27, 2004, a diverse group of companies, trade associations and public interest groups from across the political spectrum filed a Joint Statement at the Federal Communications Commission urging rejection of an FBI petition to extend controversial wiretap design mandates to the Internet.

The FBI's petition, filed March 10, 2004, asked the FCC to declare that providers of broadband access and "Voice over IP" (or Voice on the Net) services are covered by the Communications Assistance for Law Enforcement Act (CALEA). The FBI also asked the FCC to create a regulatory process under which new communications protocols, applications, or services must be reviewed and approved by the FBI and FCC before they can be deployed.

In addition to organizing and signing the Joint Statement, CDT filed its own extensive comments on April 12, 2004, and reply comments on April 27, 2004.FBI Petition to FCC for CALEA Rulemaking, Mar. 10, 2004
http://www.cdt.org/digi_tele/20040310fbipetition.pdf

Joint Statement of Industry and Public Interest, April 27, 2004
http://www.cdt.org/digi_tele/20040427jointcaleareply.pdf

CDT Comments to FCC on CALEA Petition for Rulemaking, April 12, 2004
http://www.cdt.org/digi_tele/20040412CDTCALEAComments.pdf

CDT Reply Comments, April 27, 2004 http://www.cdt.org/digi_tele/20040427cdtcaleareply.pdf

---

(2) Illegal, Unwise and Unnecessary to Apply CALEA to the Internet As both CDT's comments and the Joint Statement of Industry and Public Interest explain, the text of CALEA makes clear that it does not apply to the Internet. Congress in 1994 decided that CALEA should cover only telecommunications common carriers offering traditional wireline and wireless phone services. It does not apply to the broad category of "information services," such as Internet access, email and other on-line services.

Imposing CALEA on the Internet, and in particular imposing a prior-review requirement on new communications technologies, would destroy the ability of U.S. companies to innovate on the Internet. The Joint Statement and CDT's comments explain that such a decision would reverse more than a decade of sound policy decisions to allow the Internet to develop and grow without significant interference or constraint. Building surveillance capabilities into broadband access and Internet applications also could adversely affect privacy and open the potential for privacy abuses.

In any event, the FBI has presented no evidence of a broad problem meriting imposition of design mandates. Under existing law, the FBI already can "wiretap the Internet," and service providers regularly work with law enforcement to satisfy lawful wiretap orders quickly and fully. Service providers not subject to CALEA already have committed substantial resources to developing new technical capabilities to facilitate surveillance of advanced technologies.

In its petition and in its Reply Comments, the FBI provided no specifics about situations in which law enforcement is unable to intercept an Internet voice communication or any other Internet communication, but instead has made only vague assertions. There has been no demonstrated need to apply the failed CALEA regime to the Internet.

Further information is available at:

CDT One-Pager on the Internet and Law Enforcement Surveillance, March 19, 2004: http://www.cdt.org/digi_tele/20040315voiponepager.pdf

CDT's CALEA/VoIP Page: http://www.cdt.org/digi_tele/voip.shtml

---

(3) CALEA Is Fundamentally Broken, and Is Especially Un-suited to the InternetCALEA was adopted in 1994 in response to law enforcement concerns that wiretaps would be more difficult to implement in digital telephone networks than they had been with the analog phone system. CALEA required telecommunications common carriers to design basic wiretap capabilities into their networks. Congress specifically excluded the Internet from CALEA.

As it was implemented and interpreted by the FCC, CALEA gave the FBI very precise design control over telephone switches. CDT believes this was contrary to the intent of Congress, but over the course of a lengthy legal battle, the FBI was able to convince the FCC to mandate very specific features, including - at substantial cost to carriers and the government - features that gave the government capabilities beyond those that had been available in older phone systems.

There is now almost universal agreement that CALEA is fundamentally broken. A recent report by the Office of the Inspector General (OIG) at the Department of Justice states that ten years and half a billion dollars after enactment, CALEA compliance stands at less than 20% for wireline telephones. This is due in large part to the FBI's insistence on imposing detailed mandates on the telephone industry. After the industry worked hard to issue a standard that accommodated most of the FBI's demands, the FBI challenged the standard anyway and launched years of litigation. As CDT explained in its reply comments to the FCC, it would be an

enormous mistake to impose this broken regime on the Internet.

DOJ OIG report, "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," April 19, 2004, available at http://www.usdoj.gov/oig/audit/FBI/0419/final.pdf

---

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

CDT POLICY POST
Volume 10, Number 9, June 28, 2004

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

---

(1) Privacy Bill Passes House Judiciary Committee The Federal Agency Protection of Privacy Act (FAPPA, H.R. 338), was passed by the House Judiciary Committee on June 24. The bill includes a provision requiring federal government agencies to conduct privacy impact assessments for both new and existing agency rules and regulations.

Under the bipartisan legislation, originally introduced by Rep. Steve Chabot (R-OH) and co-sponsored by Reps. Cannon (R-UT), Boucher (D-VA) and Nadler (D-NY), a privacy impact assessment must address up front some of the basic "Fair Information Practices" reflected in the federal Privacy Act of 1974, such as notice to individuals of the collection of personally identifiable information, the right of individuals to access information about themselves, the opportunity to correct information, limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, and appropriate security measures to protect the information against abuse or unauthorized disclosure. To the extent practicable, privacy impact assessments must be made public. Significantly, the Act also provides a judicial review mechanism to ensure enforcement.

- The assessments will raise the level of attention to privacy issues within federal agencies at the initial stages of a new project or policy, before regulations are promulgated.
- The assessments will compel agencies to consider ways to reduce the privacy impact of regulations.
- The requirement that agencies invite public comment on regulations that affect privacy will bring greater transparency to the rulemaking process, allowing Congress, citizens and advocacy groups to better

scrutinize the privacy decisions of the government.
- Mandated review of existing regulations every 10 years will benefit agency operations by identifying information collection practices that have become outdated or unnecessary and that can be dispensed with altogether.

---

(3) Bill's Requirements Expand on Privacy Impact Assessments Required by the E-Government Act of 2002 The Federal Agency Protection of Privacy Act would serve as a sound complement to the E-Government Act of 2002, which requires that federal agencies conduct privacy impact assessments whenever they develop or purchase new information technology or initiate a new collection of personally identifiable information.

CDT has strongly supported the privacy impact assessment provision in both Acts and urged Congress to ensure that the two are congruent. At the markup in the House Judiciary Committee last week, Rep. Cannon introduced several significant changes to the bill to make its requirements consistent with those imposed by the E-Government Act.

- H.R. 338 as passed by the House
- CDT Executive Director Jim Dempsey's testimony on FAPPA
- E-Government Act of 2002

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

CDT POLICY POST
Volume 10, Number 10, June 29, 2004

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

---

(1) Supreme Court Reaffirms First Amendment Protection of Internet Communications In a major victory for free speech online, the Supreme Court in the case of Ashcroft v. ACLU affirmed an injunction blocking enforcement of the Child Online Protection Act (COPA). The Court's decision reaffirmed that the Internet warrants the full protection of the First Amendment. The Court wholeheartedly recognized the benefits of voluntary filtering by parents and families as an effective way to protect their children from harmful Internet content in a manner that is consistent with their own values, but still allows adults access to constitutionally protected speech.

COPA, adopted in 1998 but blocked from taking effect by lower courts, would make it a crime for anyone to make any Web communication for commercial purposes that is "harmful to minors" unless the person has used technological means to prevent access by minors (such as requiring a credit card). COPA would impose criminal and civil penalties of up to $50,000 per day for violations. CDT has opposed COPA because it threatens to chill constitutionally protected speech including a wide range of social commentary and health information.

The Supreme Court recognized that the criminal nature of COPA creates a high risk of chilling protected speech. According to Justice Kennedy, "[w]here a prosecution is a likely possibility, yet only an affirmative defense is available, speakers may self-censor rather than risk the perils of trial." When a content-based speech restriction is challenged, the government must "shoulder its full constitutional burden" to prove that the proposed alternatives will not be as effective as the challenged statute, to ensure that speech is restricted no more than is necessary to accomplish Congress' goal. The Court found that the government had not met its burden, and that filtering by parents and families was a less restrictive means of protecting children that is more effective than COPA. The Court ordered that the case be returned to the lower court for a full trial of the factual questions raised by the decision.

---

(2) Six Years of Litigation with Nothing Accomplished to Protect Children Online The Supreme Court's decision affirmed a lower court ruling that enforcement of the Child Online Protection Act should be enjoined because the statute likely violates the First Amendment.

The Supreme Court held that the Government failed to prove that the proposed alternative will not be as effective as the challenged COPA statute. Going even further, the Court opined that "[f]ilters may well be more effective than COPA."

In 1998, the district court found that COPA would violate the First Amendment because of its chilling impact on protected speech. The district court focused its opinion primarily on the argument that plausible, less restrictive alternatives to COPA are available particularly in the form of filtering technology. On appeal, the Court of Appeals also found COPA to be unconstitutional, but based its decision on a theory that the District Court had not considered. In May 2002, the Supreme Court found fault with the reasoning of the Court of Appeals, but the Supreme Court left in place an injunction against the law.

On reconsideration, in March 2003, the appellate court again ruled against the law, finding numerous constitutional problems with it. In a detailed decision, the appeals court determined that COPA would force Web publishers to block a wide range of legal material and was not the least restrictive means of protecting children online. The Justice Department appealed, bringing the case back to the Supreme Court. In its just-released opinion, the Supreme Court agreed that the District Court's 1998 decision to enjoin COPA had been correct.

Taking COPA together with the 1996 Communications Decency Act (which was struck down by the Supreme Court in 1997), Congress has spent eight years attempting to use criminal laws to censor online speech on the Internet that is lawful for adults to access. The Supreme Court's decision makes clear that this approach has been a failure.

---

(3) Court Recognizes that Education and User Control, Not Legislationn, is Key to Protecting Children
Throughout the course of the challenge to COPA, CDT has argued that the most effective way to protect children online, and the means least restrictive of free expression, is to give families and teachers resources that allow them to control what children see and do online. This approach enables the protection of children while respecting the First Amendment and the diverse sensibilities of American families.

The Supreme Court's decision reflects the findings of two major, independent studies commissioned by the Congress: the COPA Commission, a study mandated by COPA itself, and a report of the National Research Council (NRC) of the National Academy of Sciences. Both studies concluded after exhaustive research that legislation will not solve the problem of children's access to objectionable content via the Internet, but rather that technology like filtering software in the hands of parents and teachers, along with educational efforts, offer the most effective means of protecting children online.

Citing the COPA Commission directly, the Supreme Court emphasized the importance of this user control approach to guiding children's online experience. The Court acknowledged not only that the law will not solve the problem of children's access to objectionable content via the Internet, but that it is not the least restrictive means of furthering the government's goal of protecting children from objectionable content. The Court implied, however, that "Congress may act to encourage [the use of filtering and blocking technology] . . . by promoting the development of filters by industry and their use by parents."

Many Internet service providers and other companies already offer powerful filtering, blocking, and monitoring software that parents can use to protect their children from offensive material. CDT has worked with a wide

cross-section of the Internet and public interest communities to compile parental tips, filtering tools and other online safety resources at the educational site http://www.getnetwise.org

COPA now returns to the federal district court in Philadelphia for further proceedings. CDT expects to file briefs in the case, and welcomes this opportunity to demonstrate, once again, that user-based approaches remain the most effective way to protect children and respect free expression online.

The 2000 report of the COPA Commission can be found at http://www.copacommission.org/report

The NRC study, "Youth Pornography, and the Internet" (2002), is online at http://www.nap.edu/books/0309082749/html.

CDT POLICY POST
Volume 10, Number 11, July 8, 2004

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

---

(1) Anti-Spyware Measures Continue Moving Through Congress Legislation that would prohibit deceptive software is on a fast track through the House of Representatives, due in part to strong support from House Energy and Commerce Chairman Joe Barton (R-Texas). Barton recently described spyware as "a cancer on the Internet" and has predicted that an anti-spyware bill will "sometime this year become public law."

The Energy and Commerce Committee recently approved a bill that would ban certain deceptive practices and require software makers to notify consumers before collecting personal information. Lawmakers on the House Judiciary Committee have introduced a bill of their own that would establish criminal penalties for those who use spyware to steal personal information or to commit other crimes.

The Senate is also considering a bill, known as the "SPY BLOCK Act." That bill is more focused on setting notice requirements than on the prosecution of deceptive practices. Earlier this year, the Senate Communications Subcommittee held a hearing on the bill, where CDT testified that legislation might be necessary to curb spyware and that baseline privacy legislation was long overdue. The Committee has not taken further action on the spyware bill since that hearing. Although the House is currently moving rapidly, some further action by the Senate will be necessary for legislation to pass this year.

CDT strongly supports the efforts in proposed legislation to punish egregious deceptive conduct such as keystroke logging, browser hijacking, and distributed denial of service attacks with increased penalties. However, we remain concerned that, as drafted, the notice requirements in the proposed bills will actually be confusing and of little use to consumers, while serving as a potential shield for bad actors. For example, under the House Commerce bill, a software company that only uses personal information to provide a requested service and a rival company that sells information to the highest bidder must provide exactly the

same notice. The result would be that consumers are simply forced to accept all such notices in order to receive services, rendering them useless. These issues would be better addressed in a technology-neutral baseline privacy bill.

- CDT Report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem," [pdf], November 2003
- Testimony of Jerry Berman before the Senate Communications Subcommittee on "The SPY BLOCK Act.", March 23, 2004
- Testimony of Ari Schwartz before the House Consumer Protection Subcommittee on "The Safeguard Against Privacy Invasions Act." [pdf], April 29, 2004

---

(2) House "SPY ACT" On Fast Track, Clears Commerce Committee On June 24, the House Energy and Commerce Committee approved H.R. 2929, known as the "Securely Protect Yourself Against Cyber Trespass Act" or SPY ACT. The bill provides a list of deceptive software practices and would establish large civil penalties for software makers who engage in such activities. The deceptive practices list is based on a consensus document produced by the Consumer Software Working Group, which CDT convened last spring. A broad range of industry and consumer groups endorsed that document.

The bill would also require that consumers be given notices prior to the execution of adware and other software that transmits personal information. Industry groups have suggested that these provisions are overbroad and may hinder legitimate software development. Recent amendments to the bill have focused the notice requirements, and added exemptions for network security monitoring programs.

Finally, the bill includes a "Good Samaritan" provision that would remove any potential liability for providers of programs that remove or disable software in violation of the Act, provided opportunity for notice and consent are given to the user. This provision is intended to help anti-spyware technologies flourish.

CDT supports the goals of this legislation, particularly in reining in the continued bad practices of offenders. However, we remain concerned that the notice provisions will do less to make consumers aware of information collection than to further confuse good and bad practices. Since the bill covers a great deal of software, many legitimate software providers may simply add the boilerplate notice required in the bill to avoid potential liability. If the notices become ubiquitous, they will do little to help consumers distinguish software that may be of concern. At the same time, spyware manufacturers could use their compliance with the notice provision to shield themselves from liability for a variety of practices that harm consumers.

The notice provisions will also create yet another type of privacy notice in law. The specificity of the requirements assure that the privacy notices will be different than those used for financial information or medical information. For these reasons, CDT continues to believe that the notice and consent provisions of this bill would be better addressed in separate, technology-neutral, baseline privacy legislation that can streamline notices in a way that makes sense to consumers.

Finally, CDT is also disappointed that the bill provides additional enforcement authority to the FTC, but does not clearly grant the same authority to state attorneys general. The FTC alone does not have the resources to adequately enforce this legislation and state attorneys general have been consumers' first line of defense against deceptive practices. While some state attorneys general may be able to act under the bill, consumers

would be well served by a specific grant of authority.

- Text of H.R. 2929, Securely Protect Yourself Against Cyber Trespass Act
- Consumer Software Working Group Examples of Unfair, Deceptive or Devious Practices Involving Software [pdf], April 19, 2004

---

(3) House Judiciary Committee Bill Offers More Limited Approach, Criminal Penalties Three members of the House Judiciary Committee introduced their own anti-spyware legislation on June 24. HR-4661, the Internet Spyware (I-SPY) Prevention Act, would establish prison sentences of up to five years for some computer-related crimes.The I-SPY bill contains none of the notice requirements of the Commerce Committee version, but focuses instead on a narrow subset of malicious or deceptive practices. Specifically, it would make it criminal to access a computer without authorization or in excess authorization to further another criminal offense, to intentionally transmit personal information with intent to injure or defraud, or to intentionally impair security. The bill now has to pass the Judiciary Committee. It could be merged with the Commerce Committee bill or advance to the floor of the House on its own.

CDT regards the I-SPY Act as a useful supplement to the deceptive practices provisions of the Commerce Committee bill, and it avoids the issues of software-only notice requirements. Because the I-SPY bill carries criminal penalties, its focus on a narrower set of practices is appropriate. Civil enforcement is suitable for most spyware practices, but criminal provisions, which are used more rarely but carry far stiffer penalties, are appropriate for the egregious behaviors targeted by the I-SPY Act. While further tailoring of the bill is still needed-and is expected at the Subcommittee and Committee levels-its introduction is a significant step in the right direction.

- Text of H.R. 4661, Internet Spyware Prevention Act

---

(4) Prospects for Legislation Depend on Reconciling House, Senate Approaches Because few days remain in the legislative calendar, a spyware bill will have to move quickly for one to become law this year.

Reconciling or combining the two approaches currently moving in the House, the SPY ACT and the I-SPY Act, will likely be the first step. Because it has so far been less anxious to move forward with spyware legislation, the Senate remains the biggest potential obstacle to passage this year. The Senate may be more likely to act once the House has reconciled its approaches and passage of a final bill becomes imminent, but influential members of the Senate Commerce Committee have let it be known that they will not back any approach that does not have a broad consensus behind it.

Actions in the states could also accelerate the federal process. Poorly crafted state bills, or a patchwork of different bills, could provide an incentive for Congress to move forward quickly to set a uniform national standard. Spyware bills are currently pending in several states, including New York and California. Utah is the only state that has successfully passed a spyware law, but its enforcement was recently put on hold by a

state judge due to questions about its constitutionality.

- CDT Letter to Governor Olene Walker [pdf], March 12, 2004
- "Utah judge freezes anti-spyware law," CNET.com, June 22, 2004.
- For more information about spyware visit http://www.cdt.org/privacy/spyware/
- For information about how to remove spyware from your computer visit http://www.getnetwise.org/spotlight/

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