CDT POLICY POST
Volume 9, Number 13, June 30, 2003

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

---

(1) FTC Launches Do Not Call Registry The Federal Trade Commission (FTC) has just launched a new system making it possible for individuals to cut down on unsolicited commercial telephone calls. On Friday, June 27, the FTC began creating a nationwide "Do Not Call" registry. Sign up on the list, and most telemarketers will be prohibited from calling you at home, effective October 1.

Registration is now available online at http://donotcall.gov. The system was temporarily overwhelmed on Friday, when it first was announced by President Bush in a Rose Garden ceremony, but we checked this morning and it is working fine.

When you sign up, you will receive an email confirmation containing a link that you must click on to finalize entry of your phone number into the registry. If you signed up on the first day, you may not have received your confirmation until sometime over the weekend. You must follow the link within 72 hours for your registration to be successful.

The online registration is open to people across the country. A toll-free number is also available, limited for now to folks west of the Mississippi (including all of Louisiana and Minnesota). Phone registry will be open to the entire nation on July 7. The toll free number is 1-888-382-1222 (TTY 1-866-290-4236).

WARNING: Some unscrupulous companies have been offering to sign up individuals for the Do Not Call list for a fee. Please be aware that the FTC registry is a government-run service free to the public. No fee is required for this simple do-it-yourself service.

---

(2) How the Do Not Call Registry Works The FTC, the Federal Communications Commission and the states will begin enforcing the Do Not Call Registry on October 1, 2003.

Telemarketers will have to check the Do Not Call list every 90 days and stop calling those who have signed up. Companies that do not comply face fines of up to $11,000 per violation.

Consumers who register will remain on the list for 5 years, at which time they have to renew their registration. Consumers may remove themselves from the list at any time. Those consumers whose telephone number changes will also need to re-register.

Most of the 27 states that have their own do not call lists will transfer the numbers from their lists to the National Do Not Call Registry. To find out if your state is transferring its do not call list to the national registry, go to: http://www.ftc.gov/bcp/conline/edcams/donotcall/statelist.html. Consumers in states that are transferring their do not call lists to the national registry do not need to re-register.

Participation in the Do Not Call list will not eliminate all marketing calls. Consumers may still be contacted by companies with whom they have established a business relationship and companies they have affirmatively asked to hear from. Charities and political groups are exempt.

CDT encourages those who want fewer telemarketing calls to sign up for the Do Not Call registry. Tell your friends and family about this new way to exercise consumer choice.

Full information on the system is available at http://www.ftc.gov/bcp/conline/edcams/donotcall/index.html

---

(3) Does the Do Not Call Registry Have Broader Implications? The fact that 735,000 people signed up for the Do Not Call Registry by 5:00 PM on the first day of operation sends a powerful message about Americans' strong desire for effective protections against unwanted telemarketing. Certainly, the desire for effective solutions against spam is equally as strong.

Whether a Do Not Email Registry will work as well is unclear. FTC Chairman Muris has said he has "serious reservations." http://www.whitehouse.gov/ask/20030627.html Anti-spam legislation reported by the Senate Commerce Committee would require the FTC to report to Congress on the feasibility of a Do Not Email list, based on the experience with the Do Not Call registry.

It is interesting that the Federal Communications Commission, which had seemed skeptical of the Do Not Call registry, came out in favor of it, extending the rule to the telecommunications companies under the FCC's jurisdiction.

The immediate popularity of the Do Not Call registry is also generally relevant to the broader consumer privacy debate, at least as a demonstration of peoples' desire to control the use of information about themselves.

For information about other privacy issues, go to the Consumer Privacy Guide
http://www.consumerprivacyguide.org

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

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

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

---

(1) Senate Committee Approves Anti-Spam Bill On June 19, the Senate Commerce Committee approved S. 877, the CAN-SPAM ("Controlling the Assault of Non-Solicited Pornography and Marketing") Act of 2003. Sponsored by Sens. Conrad Burns (R-MT) and Ron Wyden (D-OR), the bill is one of several Congress is considering to stem the flow of fraudulent or unsolicited commercial email. Given estimates that spam constitutes as much as 50% of email traffic, chances are higher than ever that Congress will adopt a federal anti-spam law. But the final shape such legislation will take is unclear, and some of the legislative proposals pose risks to free speech and privacy values.

Spam causes problems for Internet users, service providers and legitimate marketers. Users complain of email boxes overflowing with unwanted messages, some of which contain personally offensive material. ISPs struggling to keep spam from their customers bear costs in terms of bandwidth and personnel. Legitimate marketers worry that unwanted marketing messages threaten to drown out appropriate communications with consumers.

CDT supports the enactment of federal legislation to limit spam. But it will not be easy to find an approach that responds to the sometimes disparate interests at stake while protecting freedom of speech and without limiting innovation. Final legislation will also need to consider the interests of the states in protecting the consumer rights of their citizens.

To find out more about how spammers operate, see CDT's report "Why Am I Getting All this Spam," available at http://www.cdt.org/speech/spam/030319spamreport.pdf

---

(2) CAN-SPAM Includes Criminal and Civil Provisions The CAN-SPAM bill covers all commercial email, not only that which is unsolicited, with a combination of criminal and civil provisions:

- Criminal Provision: The bill would prohibit the use of materially false or misleading header information - the information indicating the source of the message - in commercial electronic mail messages. By falsifying information, spammers make it difficult for ISPs to filter out spam. The criminal provision carries a penalty of a fine or imprisonment for up to 1 year.
- Civil Provisions: The civil provisions prohibit not only false or misleading header information, but also deceptive subject lines that are "likely to mislead" the recipient.
- Opt-out: Under the bill, commercial email would be required to contain a return address or Internet-based mechanism to allow the recipient to opt out of receiving more email. Senders of unsolicited email to someone who has opted out would incur a civil penalty.
- Aggravated violations: The bill also prohibits dictionary attacks, "harvesting" of email addresses from Web sites, automated creation of multiple email accounts, and the hijacking of computers to relay otherwise unlawful commercial email.
- Labeling: All unsolicited commercial email must include identification that the message is an advertisement or solicitation.
- Physical address: All unsolicited commercial email must include a valid physical postal address of the sender.
- Preemption: The CAN-SPAM bill would supersede state laws concerning unsolicited commercial email messages. Spammers would continue to be subject to state laws that prohibit falsity or deception in any portion of a commercial email message.
- Enforcement: In general, the law would be enforced by the Federal Trade Commission. States could bring civil actions on behalf of their residents. ISPs could bring civil actions to enjoin violation of the Act or to recover actual or statutory damages. No private right of action is provided for individuals.
- Do-Not-Mail Registry: The CAN-SPAM bill would requires the FTC to report to Congress on the feasibility or a "Do Not Mail" registry similar to the "Do Not Call" registry soon to be launched by the FTC.

CDT's full summary of the CAN-SPAM bill is at http://www.cdt.org/speech/spam/030624cdtanalysis.pdf

---

(3) Congress Must Choose Among Various Anti-Spam Proposals S. 877 is one of several proposals currently under consideration by the Congress to reduce spam.

Another Senate bill, S. 1231, introduced by Sen. Charles Schumer (D-NY), would require marking of unsolicited commercial email with an ADV label in the subject line; make it unlawful for a person to send commercial email in violation of ISP policies or terms of service; make it unlawful to send commercial email that contains false, misleading, or deceptive information in the subject line, the header or router information, or the body of the message; and establish a "Do-Not-Mail" registry. The bill would give individual users the right to sue for injunctive relief and damages of up to $1,000 per email.

Senate Judiciary Committee Chairman Orrin Hatch (R-UT) and ranking Democrat Patrick Leahy (VT) have introduced a bill, S. 1293, focusing on criminal penalties. It would criminalize: (1) hacking into a computer to intentionally send multiple commercial email messages; (2) using a computer system to relay or retransmit multiple emails with the intent to deceive or mislead recipients or ISPs as to the origin of such messages; (3) falsifying header information; or (4) falsifying registration information for multiple email accounts or domain names and using them to send multiple commercial emails. The term "multiple" would be defined as more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages

during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period. The bill imposes criminal penalties, including forfeiture, and authorize ISPs to sue injunctive relief and damages.

---

(4) House Committee Action Imminent The House Judiciary and Commerce Committees are expected to hold hearings on spam legislation immediately after the July 4 recess. The Judiciary Committee hearing is scheduled for July 8; the Commerce Committee may hold a hearing the next day. Committee markups could follow very soon thereafter.

In the House, senior Members of the Commerce and Judiciary Committees have introduced H.R. 2214, the Rid SPAM Act. It includes criminal provisions, opt-out requirements and mandatory labeling of sexually explicit material.

Another house bill is the Anti-spam Act of 2003, sponsored by Reps. Wilson (R-NM), Green (D-TX.), Boucher (D-VA), Dingell (D-MI), Markey (D-MA), and others. The Wilson-Green bill, H.R. 2515, would require all commercial email to include clear and conspicuous identification that the message is commercial in nature, an opt-out opportunity, and a valid street address of the sender. It would be unlawful to send email to consumers who had opted-out of receiving further messages from the sender or "covered affiliates." The bill would also prohibit sending commercial emails that contains false or misleading header information or subject lines. It would prohibit using harvested email addresses and dictionary attacks. It would require e-mailers sending "sexually oriented" materials to label their content and would give the Federal Trade Commission regulatory authority to prescribe the marks or notices that must be used. The bill's provisions carry both civil and criminal penalties.

A third, "compromise" bill is being drafted, which may be the preferred language at markup.

Final note: All participants in the debate must realize that no legislation will totally solve the spam problem. There is no "silver bullet." ISPs and users will continue to need to use filters and other technology tools.

In the coming weeks, CDT will be working with key stakeholders to find an effective, balanced legislative response to spam.

CDT op-ed on spam, Legal Times, June 16, 2003: http://www.cdt.org/publications/030616legaltimes.pdf

CDT's spam legislation page: http://www.cdt.org/legislation/108th/junkemail/

CDT POLICY POST
Volume 9, Number 15, July 24, 2003

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

---

(1) GetNetWise 2.0 Launched with Expanded User Empowerment Resources Useful tips and tools for protecting children online, stopping spam, keeping personal information private, and securing home computers are now available online at GetNetWise.org.

CDT has been a major supporter of GetNetWise and encourages users to take advantage of and promote this convenient resource. Sponsored by a diverse group of Internet companies and public interest organizations, and developed by the Internet Education Foundation, GetNetWise 2.0 gives Internet users the resources they need to make informed decisions about how they use the Internet.

Originally developed in 1999 to assist parents in guiding their children's online experience, GetNetWise has been expanded to cover other issues of concern to Internet users - spam, privacy and security.

The GetNetWise tools support the "user empowerment" approach to the Internet that CDT has long promoted - educating users and giving them the tools they can use to tailor their online experiences to their own values.

The expanded GetNetWise resource is at http://www.getnetwise.org.

If you would like to promote GetNetWise 2.0 or if you have tools that you want included in the resource lists, contact Megan Kinnaird at megan@neted.org or Becky Chacko becky@neted.org.

---

(2) GetNetWise 2.0 Resources Encompass Child Safety, Spam, Privacy and Security The expanded

GetNetWise offers tips, tutorials, interactive tools and downloads to assist users in securing a positive online environment. The user-friendly Web site has four content areas:

- **Keeping Children Safe Online** - Parents can learn more about the risks kids face online, search or browse for Internet safety products, browse great sites families can visit together, and learn how to identify online trouble and report problems to law enforcement.
- **Stopping Unwanted Email and Spam** - Provides information about how to reduce the amount of unwanted email, including simple tips, access to spam filtering tools, and instructions about how to report fraudulent spammers to the Federal Trade Commission.
- **Protecting Your Computer from Hackers and Viruses** - Users can find information about the risks that hackers and viruses pose to computer files and software. GetNetWise provides tips to prevent viruses from infecting software and to keep hackers from compromising computers.
- **Keeping Your Personal Information Private** - Includes a guide to tools and techniques to better control how much personal information users share with online stores, Web sites, and emailers.

The new site also includes video tutorials - animated "flash" presentations that walk users step-by-step through the process of installing or using technologies and tools.

---

(3) Expanded GetNetWise Responds to Changing Internet and its Population In 1999, at the height of the debate over Congressional efforts to censor the Internet, Internet companies and public advocacy groups saw the need for an easy-to-use and widely-promoted resource that would provide information and tools to parents wishing to protect their children from offensive content. They created GetNetWise to bring together diverse and often uncoordinated consumer education efforts. GetNetWise is now one of the most linked-to sites on the Web, with 81,000 external links.

In launching the new GetNetWise 2.0, CDT President Jerry Berman stressed that it is not intended to substitute for legislation on issues like privacy or spam, where users deserve a baseline of legal protection. "Whether or not we have laws to address these issues, consumers need access to information about their rights and responsibilities and about how they can control their online experience. Given the global nature of the Internet and the limitations of government action, user empowerment has to be part of the solution to pressing concerns like offensive content, privacy invasions, security, and spam."

The new version of GetNetWise reflects the changing Internet. While the safety of children remains central to the project, Internet users also confront the challenges of spam, protecting the privacy of personal information, and the need to maintain the security of their computers. Reflecting the emergence of the broadband Internet, the site highlights special advice and tools for users with high speed access.

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

CDT POLICY POST
Volume 9, Number 16, July 31, 2003

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

---

(1) TSA Issues Second Privacy Act Notice Expanding and Narrowing CAPPS II The Transportation Security Administration released today an interim Privacy Act Notice on its Computer Assisted Passenger Prescreening System, or CAPPS II, announcing that testing of elements of the controversial airline security program is beginning. While TSA has imposed some important privacy protections on CAPPS II, it expanded the system's mission to include catching ordinary criminals who pose no special risk to airlines and it exempted the system from a number of Privacy Act protections.

The new notice is far clearer than the one originally published in January. TSA and the Department of Homeland Security's new Privacy Officer, Nuala O'Connor Kelly, should be commended for providing significant details about the plans for CAPPS II, and for seeking further public comment. CAPPS II will not be used to actually screen passengers until further comments are considered. The Notice also acknowledges the importance of evaluating the effectiveness of the system during the testing period to decide whether to go forward with active implementation.

The Interim Notice also puts into writing some important privacy protections that TSA has been promising Congress and privacy advocates for the last several months. It confirms that TSA would rely on commercial data providers only to authenticate the identity of passengers, and that it would not use health information or credit worthiness as part of that authentication process. It also clarified that commercial data providers would not be permitted to retain any data provided to them by the government for purposes of CAPPS II.

The new Notice states that the government would retain data about a U.S. person (a citizen or permanent resident alien) only for a "certain number of days" after the person's travel has been completed -- not the 50 years indicated by the first notice. We note, however, that until recently TSA had been saying that passenger data would be purged immediately after the completion of a flight.

The new Interim Privacy Act Notice for CAPPS II is at
http://www.cdt.org/security/usapatriot/030731cappsii.pdf

For background on CAPPS II and other initiatives: http://www.cdt.org/security/usapatriot/datamining.shtml.

---

(2) Mission Creep Begins: Scope of CAPPS II Expanded Despite these important protections, CDT is concerned about the expansion of the scope of CAPPS II. According to the Interim Notice, CAPPS II would be used not only to identify individuals (including U.S. citizens) with ties to international terrorist organizations, which TSA repeatedly stated in recent months was the sole goal of CAPPS II, but also: (1) individuals with ties to domestic terrorist organizations (a category left undefined); (2) individuals with outstanding federal or state arrest warrants for crimes of violence; and (3) potentially, visa and immigration violators. Each of these expansions creates a significant danger.

The question of who is considered a domestic terrorist is not a simple one. Certainly if the Intelligence Community has specific intelligence about a threat to aviation security from a particular domestic organization, TSA should coordinate with the FBI to prevent an attack. But in the absence of such a threat, how does TSA decide who is a domestic terrorist who should be flagged by CAPPS II? Does it include anti-abortion activists who break the law by blocking access to abortion clinics or who may be organizationally or ideologically related to those who have killed doctors or committed arson at clinics? Does it include members of Earth First or other radical environmental groups that have engaged in illegal acts and have been investigated by the FBI as terrorists? By expanding CAPPS II to the realm of purely domestic terrorism, TSA will find itself having to evaluate the political activities of Americans, which is not a role it should relish.

Similarly, it is not clear that individuals with outstanding warrants for crimes of violence are a threat to other airline passengers. To the degree they are a threat to individuals after they get off the plane, that goes far beyond the scope of TSA's mission of aviation security.

In terms of immigrants, the otherwise informative Notice is unclear. One sentence states: "It is further anticipated that CAPPS II will be linked to the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program at such time as both programs become fully operational, in order that the processes at both border and airport points of entry and exit are consistent."

These additional uses of the program, no matter how compelling they might seem, would divert resources from the core mission of aviation security, thereby reducing TSA's ability to keep airline transportation safe from terrorists. The broader the mission, the higher the likelihood of mistake.

---

(3) TSA Exempts CAPPS II Program from Important Privacy Act Protections The Interim Notice exempts the CAPPS II program (and its associated "system of records") from key provisions of the Privacy Act. For example, CAPPS II would be exempt from the Privacy Act's requirement that agencies maintain only records "relevant and necessary" to accomplish their statutory purpose.

Other exemptions eliminate the possibility of judicial review of TSA's response to citizen requests for access to or correction of data used by CAPPS II. The Interim Notice exempts CAPPS II from the provisions of the Privacy Act that require agencies to provide individuals with access to certain government records and the opportunity to correct them. TSA instead proposes substituting its own procedure for individuals to request

access to CAPPS II records. But that procedure offers no opportunity for judicial review of any TSA decision to deny access to particular records.

Comments are due to TSA within 60 days. CDT will be submitting comments and urges interested citizens to do so as well.

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

CDT POLICY POST
Volume 9, Number 17, August 1, 2003

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

---

(1) CDT Calls For Accountability in Domain Names Management In testimony before a Senate Subcommittee July 31, CDT highlighted substantial accountability and legitimacy questions at the Internet's manager of important technical functions, the Internet Corporation for Assigned Names and Numbers (ICANN), calling for better progress by ICANN at meeting public interest goals.

Since 1998, ICANN has coordinated critical Internet systems like the Domain Name System (the system of names like 'cdt.org'), IP address hierarchy (computer addresses), and other globally-important functions. These systems have great importance worldwide, making ICANN's activities the subject of global interest. Throughout that time, ICANN has been the subject of much controversy regarding its structure and processes; CDT, along with many other observers of ICANN, believes that it must strive to reflect the interests of Internet users in its activities.

CDT believes that ICANN has the right basic approach to Internet management. But because the systems ICANN oversees are crucial to the Internet's proper functioning, ICANN must prove itself accountable, representative of the broad Internet community, and limited in its authority. While ICANN has made some progress in these areas, improvement is needed. In order to promote progress, CDT believes that the U.S. government's primary agreement with ICANN, the Memorandum of Understanding, be renewed in September for a term of no longer than one year.

The Subcommittee Chairman, Conrad Burns (R-MT), echoed CDT's call for better accountability at ICANN and promised continued Congressional oversight of ICANN as it continues to grow.

The testimony of Alan Davidson, CDT's Associate Director, is available at

(2) ICANN's Private-Sector Structure Remains the Right Approach CDT strongly believes that the original ICANN vision of private-sector management is still the best approach for managing the Internet's key functions. Key features of this vision include:

- Non-governmental -- Private sector bodies may more nimbly address fast-paced, complex Internet technical decisions, and may better reflect the diversity of user interests.
- Bottom-up and consensus oriented -- Decisions made in the best traditions of Internet bottom-up processes can account for broad interests and encourage compromise
- Narrowly focused -- A focused mission creates trust that ICANN would not exercise undue power and increases comfort in its non-governmental character
- Globally representative -- Helps ensure both public accountability and to include the interests of stakeholders affected by its decisions.

ICANN has made some progress in realizing this vision, but there is a significant distance still to go. Serious questions exist about ICANN's accountability, the lack of constraints on its authority, low participation and representation by key groups, and too-frequent departures from "bottom-up" decision making.

Unless ICANN can do better at realizing these pieces of its vision, it risks grave consequences. Powerful entities such as foreign governments, the International Telecommunications Union (ITU), and even the United Nations are beginning to discuss possible alternatives to ICANN. Such alternatives would likely include a vastly expanded role for governments, creating a costly and user-unfriendly environment that would poorly serve the interests of Internet users.

---

(3) CDT Proposes Metrics to Evaluate ICANN With so many challenges facing ICANN, objective assessment of its overall progress has been difficult. To date, there is no widely agreed upon set of benchmarks for measuring how ICANN is doing -- and it is unclear how ICANN itself measures success.

To assist those seeking to understand ICANN's progress, CDT has released a new study, "Assessing ICANN: Towards Civil Society Metrics for Measuring ICANN," in which we review the literature that has been published surrounding ICANN and identify key recurring themes and goals. Drawing from those recurring themes, CDT has suggested ten "civil society metrics" for assessing ICANN from a public interest perspective:

1. Stable and secure coordination of key Internet functions.
2. Adherence to clearly defined scope of activities.
3. Accountability to affected stakeholders, including effective independent review procedures.
4. Transparency, including procedural and financial transparency.
5. Representation of key Interest groups, including the public's interests.
6. Acceptance by key stakeholders, ccTLDs, Regional Internet Registries, etc.
7. Minimized impact on user rights, such as privacy and free speech; consideration of impact on Less Developed Countries, etc.
8. Support for competition and, when possible, reliance on market mechanisms.
9. Increased security of the root server system.

10. Support for long-term evolution and innovation in information and computing technologies.

CDT believes that a set of commonly agreed metrics is critical to evaluating ICANN's strengths and shortcomings. Our hope is that other groups will use this list, or create their own, to develop a multi-sectoral approach to assessing ICANN. With a comprehensive framework for evaluating ICANN in place, discussions of ICANN's strengths and shortcomings will be facilitated and progress more achievable.

"Assessing ICANN: Towards Civil Society Metrics for Measuring ICANN" is available at http://www.cdt.org/dns/icann/030731assessingicann.pdf [pdf]

---

(4) Whois Privacy a Critical Upcoming Issue for ICANN The Whois database -- a public listing of contact information for millions of domain name registrants -- has long raised significant privacy concerns. In the next year, ICANN is expected to consider reforms to Whois; its approach in dealing with this issue will be an important indicator of the state of accountability and representation at ICANN.

Currently, the registrant of a domain name in the public gTLDs and many ccTLDs must make certain technical and administrative contact information available in the "Whois" database accessible to the public online. Originally designed to allow contact in the case of a technical problem, the database is now also used by law enforcement, consumer protection agencies, and private groups including intellectual property holders.

When individual Internet users register domain names, Whois may require that they make their names, home addresses, home phone numbers, and home e-mail addresses publicly available to the world. Such potentially sensitive personal information, released publicly, can be used for unrelated purposes ranging from unwelcome marketing to identity theft, fraud, stalking, or other criminal activities. This exposure violates worldwide privacy norms and has put Whois on a collision course with national privacy laws, particularly in Europe, where is appears to violate the law of some countries.

A move is underway at ICANN to reform Whois in ways that will address individuals' privacy concerns while maintaining legitimate uses for the data. Proposals include the creation of a "tiered access" system for viewing Whois data, providing notice to users when their data is viewed, and creating "audit trails" that could expose abuse or misuse of the database. CDT believes a balance can be struck that protects privacy and allows reasonable access to data for important public purposes. ICANN's ability to incorporate the privacy interests of the global user community in this debate will be closely watched.

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

CDT POLICY POST
Volume 9, Number 18, August 5, 2003

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

As Congress heads into its August recess, CDT recaps significant legislative developments over the past few weeks related to the USA PATRIOT Act and to data mining and other government uses of commercial data, such as the Total Information Awareness and CAPPS II.

---

(1) Bills Introduced to Curb PATRIOT Act Powers

- On July 31, Sen. Lisa Murkowski (R-AK) introduced the Protecting the Rights of Individuals Act (S. 1552), a bill that would place some modest checks and balances on the most troublesome provisions of the USA PATRIOT Act. Cosponsored by Sen. Ron Wyden (D-OR), the legislation's ten provisions leave in place expanded law enforcement and intelligence powers granted by the PATRIOT Act, but ensure that privacy and other civil liberties will be better protected when the FBI and other agencies exercise those powers.

Among other limits, the Murkowski-Wyden bill would:

- guarantee that Americans' homes will not be searched in secret unless necessary;
- limit the FBI's ability to look at sensitive, personal information, including medical, library and Internet records, without demonstrating specific suspicion to a judge; and
- increase judicial review for some telephone and Internet monitoring;

The bill is available at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s1552:, and CDT's press release in support of the bill is at http://www.cdt.org/press/030801press.shtml.

- In other PATRIOT Act developments, the House of Representatives voted overwhelmingly to prohibit the FBI from spending any funds to conduct "sneak and peek" searches in criminal cases, rolling back a

part of the USA PATRIOT Act that authorized the FBI to search peoples' homes and offices without telling them until weeks or months later. Rep. Butch Otter (R-ID) offered the amendment to the Commerce-Justice-State appropriations bill; it can be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HZ00292:.

- Sen. Russell Feingold (D-WI) introduced his Library, Bookseller, and Personal Records Privacy Act (S. 1507), which would limit the FBI's ability to obtain library, medical and other sensitive personal records in an intelligence investigation without individualized suspicion. The Feingold bill can be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s1507:.

---

(2) Congress Expresses Concern About "Data Mining" As the August recess loomed, congressional members also offered several measures demonstrating concerns about government data mining and other uses of commercially available data:

- **Use of Commercial Databases**: Sen. Ron Wyden (D-OR) introduced legislation prohibiting use of funds to purchase commercial data for law enforcement and intelligence purposes unless the agency has first reported to Congress about its use of the data and the potential privacy implications. The bill, the Citizens' Protection in Federal Databases Act of 2003 (S. 1484), would also prohibit all federal agencies from conducting searches of commercial data based on purely hypothetical scenarios of future terrorist attacks. S. 1484 can be found at http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s1484:.
- **TIA**: Both the House and Senate Defense Department appropriations bills, passed in July, contain limitations on DARPA's Total (now Terrorism) Information Awareness program. The House version extends to FY2004 the Wyden-Grassley amendment barring domestic deployment, while the Senate version zeroed out funding entirely for TIA. Conference action is still pending on the final version of the bill. For more on TIA: http://www.cdt.org/security/usapatriot/datamining.shtml.
- **CAPPS II**: The Conference Report on the FAA reauthorization bill, which almost certainly will become law, blocks deployment of the Transportation Security Administration's CAPPS II airline passenger screening project until DHS certifies that the program meets certain privacy standards. It also requires both a GAO report with privacy recommendations and a report from DHS on the privacy and civil liberties implications of CAPPS II. In addition, the Senate passed an amendment to the DHS appropriations bill offered by Sen. Robert Byrd (D-WV) that would prohibit CAPPS II funding until GAO issued a report stating that CAPPS II had met certain privacy standards. For more information about CAPPS II, including the Interim Privacy Act Notice issued last week: http://www.cdt.org/publications/pp_9.16.shtml; and http://www.cdt.org/security/usapatriot/datamining.shtml.
- **DHS and Data Mining**: The Senate passed an amendment to the DHS appropriations bill sponsored by Sen. Russell Feingold (D-WI) requiring a GAO report on data mining activity at DHS.

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

CDT POLICY POST
Volume 9, Number 19, September 12, 2003

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

---

(1) Pennsylvania Attorney General Halts Secret Censorship Scheme In the face of a legal challenge brought by CDT, the Pennsylvania Attorney General agreed on September 9, 2003, to stop issuing secret censorship orders to Internet Service Providers (ISPs). The AG's concession was immediately embodied in a restraining order issued by the federal district court in Philadelphia.

During 2002 and 2003, the Attorney General had issued, without any court review or opportunity for appeal, more than 300 blocking orders directed at more than 700 Internet web sites that the AG asserted contained child pornography. Although the fight against child pornography is very important, the blocking orders also had the effect of blocking access to innocent web pages that have no relationship with child pornography. Because of the technical design of the Internet (as discussed below), a far more effective way to combat child pornography would be to go after those who create and post the material, rather than the ISPs who have no knowledge of, or relationship with, those individuals.

---

(2) AG's Action Comes in Response to Legal Challenge Filed by CDT, ACLU

On September 9, 2003, CDT together with the ACLU of Pennsylvania and Plantagenet, Inc., a Pennsylvania

ISP, filed a constitutional challenge to a Pennsylvania statute that blocks access to Internet sites accused of carrying child pornography and that results in the blocking of wholly innocent websites.

The challenge, filed in the U.S. District Court of the Eastern District of Pennsylvania, argues that the Pennsylvania law is a prior restraint on speech that violates the First and Fourteenth Amendments and the Commerce Clause of the Constitution. The Pennsylvania law, passed by the state legislature in early 2002, imposes potential liability on Internet Service Providers 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. The law makes any ISP doing business in Pennsylvania potentially liable for content anywhere on the Internet.

The law provides that the state Attorney General or any county district attorney can unilaterally apply to a local judge for an order declaring that certain Internet content may be child pornography, and requiring any ISP serving Pennsylvania citizens to block the content. The entire court proceeding occurs with only government participation and no prior notice to the ISP or the Web site owner, violating the due process and prior restraint protections of the Constitution. The technical design of the Internet dictates that most ISPs can only comply with the blocking orders by also blocking a significant amount of wholly innocent web site content as well.

The Pennsylvania Attorney General has gone further, bypassing the law's inadequate court procedures by simply issuing orders to ISPs to block content. These orders are totally secret, and the Attorney General has refused to comply with "Right to Know" law requests for the content of the secret orders.

---

(3) The Statute and Censorship Orders Raise Legal and Technical Problems

The Pennsylvania law raises very serious problems - legal and technical. The law and the AG's secret blocking both violate constitutional principles of free speech and due process. Compliance with the law also requires that web sites completely unrelated to any child pornography sites also be blocked, simply because most Internet web sites today share their "Internet Protocol" (or "IP") addresses with many other wholly unrelated web sites.

The magnitude of over-blocking under the Pennsylvania law is demonstrated in a report issued 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 addition, the law also forces ISPs to manipulate the sensitive "routing tables" used to send communications around the Internet, increasing the risk of major Internet service outages.

Copies of the complaint filed by CDT and the ACLU, as well as the Memorandum in Support of a Motion for a Temporary Restraining Order and other background information, is available online at http://www.cdt.org/speech/pennwebblock/.

---

(4) Child Pornography Deserves Focused and Effective Law Enforcement Efforts

CDT shares the belief that child pornography has no place in any civilized society, and supports the vigorous prosecution of those responsible for the creation of such material.

The Pennsylvania statute challenged by the lawsuit seriously restricts lawful Internet content and harms the technical operation of the Internet itself. But the law does nothing to remove the child pornography at its source or to prosecute the creators and posters of the content. It does, however, set a dangerous precedent of regulating ISPs and other intermediaries without notice to the publishers who might be affected.

There are a wide range of less constitutionally damaging but more effective alternatives available to government to combat child pornography, including directly contacting the Web Host (or hosting ISP) about the alleged child pornography, to seek to have the content removed at the source, and working with national and international investigators, including the Federal Bureau of Investigation and the U.S. Customs Service, to investigate and prosecute the creators and knowing distributors of child pornography. In contrast to those approaches that directly target the child pornography and its makers, the approach used in Pennsylvania actually allows the child pornography to continue to circulate on the Internet.

---

(5) Next Steps in the Litigation

In addition to entering the agreed Temporary Restraining Order halting the secret censorship scheme of the Attorney General, the Court also ordered that the litigation proceed on an expedited schedule. The parties have started a period of discovery, and in early November CDT and the ACLU will file a motion to have the statute itself declared to be unconstitutional. The Court has set a hearing on that motion for November 21, 2003.

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

CDT POLICY POST
Volume 9, Number 20, October 17, 2003

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

---

(1) Senators Question Rumsfeld on Privacy Act Violations in JetBlue Case In the latest reaction to airline JetBlue's disclosure of passenger records to the Army, Senators Joseph Lieberman (D-CT), Susan Collins (R-ME), and Carl Levin (D-MI) called on Defense Secretary Donald Rumsfeld to investigate whether the Army violated the Privacy Act by not informing the public of the collection of data from JetBlue Airlines and other sources.

Under the Privacy Act, new government databases generally cannot be created in secret. CDT believes that the Army should have issued a public notice that it was acquiring airline passenger records. That would have given members of the public and Congress an opportunity to ask why.

The Army and JetBlue have defended their secrecy by arguing that the government never acquired the data -- JetBlue turned it over to an Army contractor, Torch Concepts. However, Section (m) of the Privacy Act states that the requirements of the Act apply even when the government contracts out data collection or analysis to a private company. The senators are asking the Army a series of questions, including how the access to JetBlue data was relevant to the Army's mission.

Lieberman/Collins/Warner/Levin Letter to Secretary Rumsfeld: http://www.cdt.org/privacy/031017rumsfeld.pdf

---

(2) Background on the Sharing of Commercial Flight Passenger Data with the US Army In September,

JetBlue confirmed reports that it had violated its privacy policy by sharing passenger information, including names, addresses, phone numbers and itineraries, with Torch Concepts, a contractor for the US Army working on military base security systems.

Torch Concepts used the passenger information to populate a prototype database. Torch then used data aggregator Acxiom Corporation to authenticate the identities of passengers and to add to each record more personal details such as public record information. Few details have been made public about the project, but Torch Concepts had been promoting it and posted a PowerPoint presentation describing its work that included detailed information about a specific passenger (without the passenger's name).

It is believed that the Transportation Security Administration (TSA), then housed at the Department of Transportation but since moved to the Homeland Security Department, facilitated the arrangement between JetBlue and the Army's contractor. Early reports speculated that the passenger information was being used for the Computer Assisted Passenger Pre-Screening System (CAPPS II), but it now appears that the effort was unrelated to airline security and that TSA and TSA contractors never received the information in question.

Wired story, 9/23/03, "Army Admits Using JetBlue Data":
http://www.wired.com/news/privacy/0,1848,60540,00.html

New York Times Editorial, 9/23/03, "Betraying One's Passengers" (subscription required):
http://www.nytimes.com/2003/09/23/opinion/23TUE2.htm

---

(3) FTC, DHS Privacy Officer Investigating The Federal Trade Commission has confirmed that it is investigating JetBlue's actions in the incident based on a complaint filed by privacy groups.

On September 22, the Electronic Privacy Information Center filed a complaint with the Federal Trade Commission. The complaint charges that JetBlue violated its own privacy policy, which would considered a deceptive practice under the Federal Trade Commission Act. The complaint also calls Acxiom's practice of providing personal information to Torch without consumer notice or consent an unfair practice under the Act. The Commission has acknowledged that it is investigating JetBlue based on the complaint.

EPIC Complaint: http://www.epic.org/privacy/airtravel/profiling/jetblue/ftccomplaint.html

Nuala O'Connor Kelly, Chief Privacy Officer for the Department of Homeland Security, has also announced that she plans to investigate any role that the Transportation Security Administration may have played in the incident.

The DHS Chief Privacy Officer position was created by Congress in the Department of Homeland Security Act. Kelly has said publicly that she would like to be seen as having some independence to work within the agency. This investigation will test the amount of independence and influence that she will be able to exercise.

---

(4) JetBlue Case Illustrates Ongoing Concerns with Commercial Data The JetBlue case suggests how widespread is the government's current use of commercial data. While many were focused on DARPA's Total Information Awareness program and CAPPS II, no one had even guessed that the Army was testing whether

it could mine airline passenger lists looking for terrorists. The case gives heightened urgency to legislation introduced by Sen Ron Wyden (D-OR), which would require all government agencies to report publicly on their use of commercial databases for data mining. We simply do not know how many other agencies are acquiring, or using contractors to acquire, commercial databases.

The case also highlights the limitations of current privacy laws. Airlines can voluntarily disclose passenger records to the government or its contractors because there is no law protecting travel data or many other categories of electronic data. (JetBlue almost certainly violated the FTC Act by disclosing the data in violation of its posted privacy policy, but it is perfectly legal for any airline or car rental agency or merchandiser to say in its privacy policy that it provides information to the government when appropriate to assist in legitimate government functions or some similarly broad caveat.)

CDT has argued that there is a need for clear, government-wide rules on data-mining and other government uses of commercial databases. The starting point for these rules are the long-accepted Fair Information Principles of Notice, Choice, Collection Limitation, Use and Disclosure Limitation, Retention Limitation, Data Quality and Security, Access and Redress.

Wyden legislation: http://www.cdt.org//legislation/108th/wiretaps/#s1484

CDT testimony on data mining, July 22, 2003: http://www.cdt.org/testimony/030722dempsey.shtml

---

CDT POLICY POST
Volume 9, Number 21, November 5, 2003

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

---

(1) FCC approves digital broadcast content protection rule The FCC approved a broadcast flag rule yesterday, incorporating several consumer- friendly improvements to an earlier Motion Picture Association of America (MPAA) proposal, but leaving some major consumer concerns unanswered. The ruling will require all equipment sold after July 1, 2005 that is capable of receiving digital television (DTV) broadcasts to include approved copy protection technologies.

The broadcast flag ruling is designed to address the problem of indiscriminate redistribution of digital broadcasts online. Online piracy of television programs and movies broadcast over the air represents a significant prospective threat to the video content industry. However, the FCC's rule is of concern because it creates a government enforced technological mandate for all equipment capable of receiving and using DTV broadcasts, including computers. Such technology mandates raise extremely difficult issues regarding innovation and the way consumers might reasonably record, use, and watch television programming in the future.

Prior to the FCC's ruling, CDT released a public interest primer on the implications of the broadcast flag, which raised many of these issues and which can be found at http://www.cdt.org/copyright/broadcastflag.pdf.

The FCC ruling is at http://www.cdt.org/copyright/031104fcc.pdf.

---

(2) Broadcast flag debate has far reaching consequences for consumers The broadcast flag proposal has emerged as one of the focal points in the digital copyright debate. Creators of television programming and movies view the broadcast flag as essential to protecting high-quality content distributed through unprotected digital television broadcasts. Critics of the flag proposal view it as a dangerous precedent for government restrictions on computers and on otherwise lawful consumer uses of content.

The FCC launched its inquiry into protection of DTV broadcasts in August of 2002. Last December, the MPAA and other proponents submitted a specific proposal for a system of broadcast flag regulations. After an extended comment and review period, in which organizations and members of the public submitted over 5000 comments on the proposal, yesterday the FCC gave its approval to a broad flag rule based on the MPAA's plan.

The broadcast flag protection scheme is composed of two parts: a relatively uncontroversial technical method for marking digital television programs for copy protection, and a set of much more contentious proposed regulations for all devices that would handle flagged programs, including computers.

Yesterday's ruling outlines initial regulations about what kinds of technologies will be permitted to handle flagged DTV content, what consumer uses of flagged content will be permitted, and how specific technologies can become certified to handle flagged content.

---

(3) Flag ruling fixes some problems, but fails to address many of the hardest issues The FCC's ruling has incorporated several significant improvements over the MPAA's initially proposed rule. These include:

- explicitly allowing software-based protection technologies;
- attempting to specify objective functional criteria to be used in the initial review of protection technologies;
- clarifying that the flag rule is designed only to help curtail indiscriminate redistribution of video content online and is not intended to restrict any other forms of copying; and
- adopting an ordinary-user standard for resistance to hacking, rather than expecting certified protection to stop all committed hackers.

At the same time, several problems still remain:

- While the commission's report states that no new equipment will be needed by consumers to comply with the flag ruling, new technology that is compliant with the rule is unlikely to be compatible with devices now in consumers' homes, potentially requiring extensive, expensive upgrades.
- The FCC declined to prohibit use of the flag protections on news or public affairs content. Limitations on the ability to easily share public affairs and public domain content raise significant first amendment issues for end users.
- Of especial concern, the FCC ruling leaves many of the hardest problems up in the air. Critically, it still remains unclear what technologies and consumer uses will ultimately be permitted under the ruling and what the permanent process for approving copy protection technologies will be.
- Additionally, as noted below, the ruling sets a troubling precedent for FCC regulation of computing architecture with little clear sense of the limitations on that authority.

A good deal more work remains to be done by policy makers on the flag issue. The FCC has started a further notice of proposed rulemaking on key outstanding issues. The FCC ruling may also be challenged in the

courts and taken up by Congress.

---

(4) Flag report implicates broader copyright themes More broadly, the broadcast flag rule represents a troubling precedent for direct FCC regulation of the architecture of digital devices. The effect of the flag on innovation and on the computer remains a serious concern.

In testimony before the Senate Commerce Committee in September, CDT articulated the view that it makes sense to pursue enforcement of existing powerful copyright laws, consistent with due process and user privacy, before enacting new laws or regulations, including technological mandates.

In general, CDT has argued that the most effective way to combat illegal distribution of content over the Internet in the long-run is to compete with it, especially when attractive, legitimate services like Apple's iTunes are paired with selective well-publicized enforcement actions and broad education efforts.

The broadcast flag ruling is the first step in what is likely to be an extended debate over the appropriateness of technological mandates as a solution to copyright concerns. CDT remains active in these discussions and encourages the public to make its voice heard.

CDT testimony on copyright issues, September 2003: http://www.cdt.org/testimony/030917davidson.shtml.

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

CDT POLICY POST
Volume 9, Number 22, November 19, 2003

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

---

(1) CDT Analyzes Spyware Issue and Proposed Solutions, Launches Online Action CDT today released a report entitled "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem," addressing the growing problem of so-called "spyware" programs. The applications commonly grouped under the term "spyware" range from targeted advertising programs to more invasive key stroke loggers and screen capture utilities that can be used to steal passwords and aid identity theft. These programs pose a threat to privacy and compromise users' control over their own computers.

CDT's report describes the variety of spyware applications that exist and evaluates solutions to the spyware problem. The report reviews pending legislation and also gives users advice about steps they can take to combat these programs today.

In conjunction with the report, CDT has begun a campaign on its website calling on Internet users to send in their experiences with specific "spyware" products, so that CDT can collect the most egregious cases and file a complaint with the Federal Trade Commission.

CDT's report "Ghosts in Our Machines: Background and Policy Proposals on 'Spyware'" can be found at http://www.cdt.org/privacy/031100spyware.pdf.

CDT's call to Internet users for their spyware "horror stories" can be found at http://www.cdt.org/action/spyware/.

---

(2) CDT Report Emphasizes Control Dimension of Spyware Issue CDT's report details the significant privacy concerns raised by spyware while highlighting the larger issues raised by these applications of transparency and user control. These larger problems are sometimes overlooked in discussions about the issue and to a certain extent obscured by the term "spyware" itself.

CDT's report focuses on so-called "adware" and other similar varieties of spyware that often piggyback on free downloads, and which are increasingly the target of legislative and regulatory proposals. Users are typically unaware that these programs are being installed on their computers, and often unable to uninstall them. Even in cases where these applications transmit no personally identifiable information, they are often responsible for significant reductions in computer performance and system stability, and their unauthorized use of users' computers and Internet connections threatens the security of computers and the integrity of online communications. Arguably, a better term for many these applications would have been "trespassware."

By focusing on the range of bad practices employed by the various kinds of spyware, CDT's report emphasizes that the concerns with these invasive applications are not limited to their violations of user privacy.

---

(3) Currently Proposed Spyware Legislation Imprecise, Fails to Address Significant Issues In its report, CDT reviews two pieces of legislation that have been introduced as targeted responses to the spyware problem by Representative Mary Bono (R-CA) and Senator John Edwards (D-NC), as well as a broader online privacy bill introduced last year by Senator Ernest Hollings (D-SC), which includes a spyware component.

CDT believes that because the term "spyware" is broad and imprecise, it will be very hard to craft a definition that is exact enough for use in legislation. Based on what we have seen in currently proposed legislation, we believe the most effective approach to spyware is likely to be in the context of general privacy legislation, such as the Hollings bill.

At the same time, even considering the issues associated with spyware in isolation, legislation introduced to date has been an incomplete solution to the problem insofar as it has focused primarily on the privacy dimension of spyware. CDT argues that a full solution to spyware must deal with the user-control aspects of the issue, such as piggybacking and avoiding uninstallation. Combating these technologies will require a combination of legislation, anti-spyware tools, increased user-awareness, and self-regulatory practices.

---

(4) CDT Requests Spyware Stories for Potential FTC Complaint While a legislative approach is under consideration, CDT recommends that existing law be used to address the most egregious cases of spyware. CDT believes that some varieties of spyware may qualify as unfair or deceptive under Title 5 of the Federal Trade Commission Act, which would give the FTC authority to act against those programs.

Spurred by what it found in preparing the report, CDT is launching a campaign to solicit stories from Internet users who may have been deceived or treated unfairly by spyware. CDT plans to compile the reports, test the programs, and file specific complaints with the FTC where warranted.

Again, users can submit their spyware "horror stories" to CDT at http://www.cdt.org/action/spyware/.

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_9.22.shtml.

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

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

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

---

(1) Congress Sends Spam Bill to President for Signature On December 8, 2003, the U.S. House of Representatives passed by unanimous consent an amended version of S. 877, the "CAN-SPAM Act," sponsored by Senators Conrad Burns (R-MT) and Ron Wyden (D-OR). The Senate on November 25 had passed identical language, so the action by the House clears the legislation to be sent to the President, who is expected to sign it.

The final version of the bill sets rules for commercial email and makes no distinction between solicited and unsolicited messages. It does not prohibit unsolicited email. Rather, it prohibits certain deceptive practices and requires every commercial email message to provide an opt-out option and meet certain disclosure rules. The bill does not generally apply to "transactional or relationship messages" - such as messages that facilitate or complete a transaction already in progress or that deliver goods or services, including product updates, to existing customers.

The CAN-SPAM Act imposes criminal sanctions for use of materially false or misleading header information in commercial email messages, with fines or imprisonment. The civil provisions also prohibit false or misleading header information as well as deceptive subject lines that are likely to mislead a recipient. In addition, the civil provisions require that commercial email disclose certain specified information and provide recipients an opportunity to decline to receive any additional messages.

One troublesome aspect of the bill is a labeling requirement for all messages containing sexually explicit material. The law requires the Federal Trade Commission to specify marks or notices that will facilitate filtering of sexually oriented material, thereby inserting, in a small way, a federal agency into the design of an Internet technology.

While CDT hopes that the bill will be effective in stemming the flood of spam into users' mailboxes, it is clear

that filtering technologies and careful online behavior on the part of users will be more effective in giving users control over unwanted commercial email.

For a copy of S. 877 as passed by Congress, go to http://www.cdt.org/legislation/108th/junkemail/

To learn more about what users' can do to avoid spam, see CDT's report "Why Am I Getting All This Spam," available at http://www.cdt.org/speech/spam/030319spamreport.shtml

---

(2) CAN-SPAM Includes Criminal and Civil Provisions The CAN-SPAM bill covers all commercial email, not only that which is unsolicited, with a combination of criminal and civil provisions:

- **Criminal Provision**: The law will prohibit the use of materially false or misleading header information - the information indicating the source of the message - in commercial electronic mail messages. By falsifying such information, spammers make it difficult for ISPs to filter out spam. The criminal provision carries a penalty of a fine or imprisonment for a period of up to 5 years.

- **Civil Provisions**: The civil provisions prohibit not only false or misleading header information, but also deceptive subject lines that are "likely to mislead" a recipient.

- **Opt-out**: The bill requires in all commercial email a return address or Internet-based mechanism to allow recipients to opt-out of receiving more email. Senders of email to someone who has opted out would incur a civil penalty.

- **Aggravated violations**: The bill also prohibits dictionary attacks, "harvesting" of email addresses from Web sites, automated creation of multiple email accounts, and the hijacking of computers to relay otherwise unlawful commercial email.

- **Labeling**: All unsolicited commercial email must include somewhere in the body of the message identification that the message is an advertisement or solicitation.

- **Labeling for "sexually oriented material**:" The bill requires FTC regulated marks or notices in the subject heading of any commercial email that contains sexually explicit material.

- **Physical address**: All unsolicited commercial email must include a valid physical postal address of the sender.

- **Preemption**: The CAN-SPAM bill supersedes state laws concerning unsolicited commercial email messages, including California's opt-in law, which was due to take effect on January 1. Spammers will continue to be subject to state laws that prohibit falsity or deception in any portion of a commercial email message.

- **Liability**: The bill makes companies responsible for email sent on their behalf.

- **Enforcement**: In general, the law will be enforced by the Federal Trade Commission. States can bring civil actions on behalf of their residents. ISPs could bring civil actions to enjoin violation of the Act or to recover actual or statutory damages. No private right of action is provided for individuals.

- **Do-Not-Mail registry**: The CAN-SPAM bill requires the FTC to report to Congress on the feasibility of a "Do Not Mail" registry.

- **Studies on rewards for information about violations and on ADV labeling**: The Act requires that the FTC report to the Congress about a system for rewarding those who supply information about violations of the statute. It also requires that the FTC set forth a plan for requiring commercial email to be identifiable through use of an "ADV" or similar label in the subject line.

The Act takes effect (with the exception of the "do-not-spam registry") on January 1, 2004.

CDT's detailed summary of the CAN-SPAM bill as passed is at
http://www.cdt.org/speech/spam/031211cdt.pdf [pdf]

---

(3) CAN-SPAM May Help Curtail Spam, but Bill Has Some Troubling Provisions With the exception of the labeling requirements, CDT supported in principle the core provisions of the CAN-SPAM Act as appropriate but limited steps in addressing spam. The bill may indeed have some positive effect in slowing the growth of spam, if not actually reducing it. The bill should help ISPs filter spam and sue spammers. Prohibitions on dictionary attacks and harvesting could also be meaningful. We expect that the FTC and some state Attorneys General will diligently use the enforcement mechanisms and will be open to consumer complaints.

From a consumer perspective, the opt-out provision is useful with respect to legitimate companies. However, CDT advises users not to exercise an opt-out if they are not sure of the legitimacy of the sender - otherwise, users may just be confirming to an outlaw spammer that their email address is valid.

Clearly, passage of this legislation is only one step in the effort to curtail spam. As discussed in the CDT study, "Why Am I Getting All This Spam?," effectively stemming the flow of spam will still depend on consumer awareness of the online behaviors that spammers exploit and effective use of filtering technologies by users and ISPs.

CDT is concerned that the CAN-SPAM Act lacks what might have been the most effective means of enforcement - a narrowly drawn individual right of action. We had recommended an approach that would have allowed individuals to bring claims in small claims court involving no burdensome discovery and no class actions. Congress did not include such a provision.

Given the difficulties of enforcing inconsistent state laws on the Internet, CDT supported federal preemption of inconsistent state spam laws. But we did so recognizing that the effect of the CAN-SPAM Act on the amount and nature of spam is highly uncertain. Therefore, we recommended a mechanism to force Congress to revisit the issue substantively. We felt that the best way to do this would have been with a sunset of the preemption. If the preemption provision were to have sunsetted in three to five years, Congress would have been required to formally confront the question of whether the bill was effective. As it is, if this law does not stem the tide of spam, Congress will still face public pressure to pass more effective provisions or open the issue again to state regulation.

Finally, we are concerned about how the provisions on falsified or concealed header information could be interpreted. On balance, however, we think that it would be unreasonable to interpret the statute as prohibiting use of non-spoofed pseudonymous email addresses even for multiple commercial emails. CDT raised some of these concerns in a letter to the House Commerce Committee on Oct. 15, 2003:
http://www.cdt.org/speech/spam/031015cdt.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_9.23.shtml.

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

CDT POLICY POST
Volume 9, Number 24, December 17, 2003

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

---

(1) CDT Releases Updated Analysis as FCC Flag Rule Moves Forward The FCC broadcast flag rule, an attempt to address concerns about piracy of digital television by mandating copy protections in consumer devices, was officially published in the Federal Register earlier this month, opening the way for legal challenges and launching a follow-on proceeding in which the FCC will take up issues deferred in its first ruling. CDT has released a new report examining the flag regulation that details the concerns it raises for consumers and Internet users.

The flag regulation presents a novel policy approach, mandating that all equipment capable of receiving digital television (DTV) broadcasts include federally approved copy protection technologies. While aimed at addressing a serious copy protection issue for content owners, the flag approach also has the potential to impact how consumers will record, watch, and use digital television for many years to come--and to set a precedent for government regulation of the architecture of computers.

The Implications of the Broadcast Flag: A Public Interest Primer (Version 2.0), updates CDT's earlier report on the broadcast flag proposal and provides a detailed examination of the flag regulation put in place by the FCC. The report concludes that the FCC's ruling includes some consumer-friendly modifications to earlier proposals, but that the Commission put off consideration of many of the most important questions of concern to consumers. CDT's report notes that the Commission's ruling is unlikely to be the final word on the flag issue, as critical issues remain for a follow-on rule-making, and court challenges to the flag rule and further Congressional debate are expected as well.

CDT's updated and expanded public interest primer on the broadcast flag issue can be found at http://www.cdt.org/copyright/031216broadcastflag.pdf.

A shorter overview the broadcast flag scheme can be found at http://www.cdt.org/copyright/031200cdt.shtml and more information about digital copyright issues generally is available at CDT's digital copyright page, http://www.cdt.org/copyright/.

---

(2) FCC Ruling Includes Consumer-Friendly Changes, But Defers Key Questions The FCC's Report and Order on digital broadcast content protection, published in the Federal Register on December 3, creates a new federal regulation setting in place the broad outlines of the broadcast flag protection mechanism for digital television (DTV) broadcasts. The ruling requires that by July 2005 any new device sold or distributed in the U.S. that is capable of receiving DTV broadcasts must look for a flag that marks content as protected, and must obey certain content protection rules for flagged programs.

While the FCC ruling includes important improvements over earlier drafts of the rule proposed by the Motion Picture Association of America (MPAA) and others (see CDT Policy Post 9.21), it leaves consumers with no guarantees that many of their biggest concerns will be addressed.

A central issue in the broadcast flag approach is what protection technologies will be mandated in consumer devices and what those technologies will allow people to do. The FCC ruling appears to limit the scope of earlier proposals by seeking protection technologies that prevent indiscriminate redistribution of [digital broadcast television] over the Internet or through similar means. The rule also adds consumer-oriented factors to the considerations that will be used in the review of protection technologies. The Commission also indicated its willingness to consider software-based protection measures, which will be essential if computers are to be allowed to handle DTV content without major redesign.

However, the FCC's rule leaves unanswered the essential questions of exactly what consumers will be permitted to do with television broadcasts, and how approved protection technologies will be selected. Without answers to those questions, the ruling leaves consumers at risk that their ability to record, watch, and use television programs will be unreasonably restricted. It also leaves real concerns that the approval process for new technologies will harm innovation in new consumer products.

The FCC ruling set in motion a second rule-making proceeding designed to address many of these hard issues. The rule sets forth an interim procedure that the Commission has adopted for approving technologies in the short term, but defers the standards for a permanent approval process to the follow-on proceeding. Other questions deferred by the Commission include the effect of the Commission's rule on open source software for handling DTV broadcasts, and the definition of a personal digital network environment within which redistribution of protected content would be allowed.

Public comments are now due by January 14, 2004 in the FCC's further proposed rulemaking on the broadcast flag.

---

(3) Questions Raised About FCC Jurisdiction in Flag Ruling Credible questions have also been raised about whether the FCC had the authority to issue the flag regulation. In many ways the flag ruling creates an unprecedented level of FCC regulation of consumer electronics devices and computers, which will be directly impacted by the requirements that only authorized technologies may handle marked DTV broadcast content.

Critics have noted that the Commission has no direct statutory authorization to enact the rule, but the FCC argues that the regulation falls under its ancillary jurisdiction to promote the nation's transition to digital

broadcast. Supporters of the flag scheme have said that without some form of mandated content protection, studios and programming providers will be unwilling to release high quality content for digital broadcasts, leaving little incentive for consumers to purchase the DTV receivers that they will need if the US is to make the transition to digital.

The new version of CDT's flag primer includes an overview of the contentious jurisdiction issue, which could quite possibly be the grounds of a court challenge to the FCC's ruling. If legal challenges succeed in stopping or slowing the flag, further action may be needed by Congress to give the broadcast flag effect.

---

(4) Next Steps: CDT Urges People to Stay Involved Policy makers have generally avoided government mandates of specific Internet and computing technologies, for fear such mandates could burden the rapidly evolving information infrastructure and threaten innovation. Without changes, CDT believes the broadcast flag rule may set a troubling precedent for government regulation of the architecture of digital devices without adequate attention to the concerns of consumers and computer users.

Critical questions remain to be answered by the FCC as it continues its rulemaking on the flag approach. CDT urges those interested to file comments in the FCC's follow-on proceeding. CDT's own list of recommendations for ways the Commission can address problems with the flag approach can be found in our Public Interest Primer. Comments can be filed online at the FCC's website at http://gullfoss2.fcc.gov/ecfs/Upload/ until January 14th. The broadcast flag is MB Docket Number 02-230.

The flag issue may also come under further Congressional review, especially if legal challenges to the FCC's ruling are successful. The broader question of whether government should get directly involved the design of technologies to promote content protection is certain to remain an important issue before Congress for years to come.

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