

The Internet in Transition

A Platform to Keep the Internet Open, Innovative, and Free

June 2008 – Version 1.0

This document examines a broad range of issues the next President and Congress must address in order to keep the Internet a powerful engine for innovation, economic growth and democratization. The policies outlined in this paper describe current threats to the Internet and then proposes policies and actions that the next President and Congress should take to protect innovation, privacy, consumer choice, and freedom of expression.

This document is a work in progress. Help us refine this policy blueprint by offering feedback, suggesting changes, or simply sharing ways to make the document more effective at our Election 2008 Web site (cdt.org/election2008/). By the time a new President is elected, this document will be finalized and presented to the new administration as a transition document.

Preserving Free Speech and Protecting Children Online.....	3
Protecting Consumer Privacy in the Digital Age	6
Restoring the Balance between Security and Liberty.....	9
Promoting Global Internet Freedom	15
Keeping the Internet Open to Innovation.....	17
Promoting Open Government	21
Appendix: What Every Candidate Needs To Know About the Internet	24
Appendix: Comments to CDT's Internet in Transition: Election 2008.....	28

The next President and the next Congress should pursue policies that keep the Internet open, innovative and free, so that it can continue to expand as a platform for community, commerce, and communication.

In only a few decades, the Internet has become a powerful engine for innovation, economic growth and democratization. It is giving citizens a stronger voice in civic life and is improving government transparency. It empowers innovators, activists and researchers to communicate and collaborate with colleagues around the world. It is transforming commerce, education, culture, health care, and political discourse. Candidates are benefiting from today's Internet to build networks of supporters, raise unprecedented funds from small donors, and educate the public on their policies and visions.

Ordinary Americans are expressing their views, organizing their communities, and engaging in political debate on social networking sites and blogs.

However, these benefits of the digital revolution are not guaranteed. The next President of the United States and the Congress that convenes in January 2009 will face a series of policy challenges that threaten the future of the Internet and the opportunities it offers.

The Internet's remarkable success is built on a policy framework based on the principles of **openness, competition, innovation, non-discrimination, privacy, consumer choice and freedom of expression**. Faced with legitimate concerns ranging from terrorism to the protection of children online, policymakers must find solutions that reinforce — rather than undermine — these core principles.

This paper outlines threats to the Internet and proposes policies and actions that the next President and Congress should take to protect openness, innovation, privacy, consumer choice, and freedom of expression. Specifically, we recommend that the next President and Congress —

- Defend the Supreme Court ruling that affords the Internet the highest level of constitutional protection for free speech.
- Make education and user empowerment rather than censorship the centerpiece of federal efforts to protect children online.
- Nominate and confirm to the Federal Trade Commission individuals who will strongly promote online privacy.
- Work together to enact comprehensive consumer privacy legislation.
- Ensure strong protections for personal health information as adoption of health information technology accelerates.
- Restore checks and balances on government surveillance.
- Update protections afforded by America's communications privacy laws, to keep pace with advances in technology.
- Foster innovation and free speech with policies that preserve and enhance openness and non-discrimination on the Internet.
- Nominate and confirm to the Federal Communications Commission and other agencies individuals who will preserve the open Internet and oppose technology mandates.
- With respect to digital copyright, promote balanced approaches that both protect the rights of creators and preserve the Internet's potential to facilitate interactivity, innovation, and collaboration.
- Pursue broadband deployment and spectrum allocation policies that will facilitate expanded opportunities for high-speed Internet connectivity.
- Make the next Administration and the next Congress the most open in American history by reinvigorating the Freedom of Information Act and

using technology to make more government information available online.

- Actively promote global Internet freedom as an integral part of U.S. foreign policy.

▣ Preserving Free Speech and Protecting Children Online

The Internet has proven to be one of the greatest tools of human expression in history. Americans enjoy the strongest free speech rights on the Internet of any country in the world. However, over the past decade, policymakers eager to protect children from inappropriate content or dangerous contacts have proposed a range of measures that would stifle speech and innovation and restrict access to lawful content and constitutionally protected speech.

Although children should be protected online as well as off, censorship laws and measures that place web operators in the role of gatekeepers interfere with constitutionally protected speech and are not effective ways to improve children's online safety. Instead, governmental efforts should aim at empowering and educating parents and children about smart online behavior, providing them with the filters and other tools that can guide a child's online experiences.

Ill-considered censorship measures and technology mandates aimed at child protection would seriously discourage innovation online and stifle the dynamic and economically important evolution of technology that we have witnessed over the past 15 years. Children can be protected without interfering with the development of new online applications and services.

The next President and Congress should —

- **defend the Supreme Court ruling that affords the Internet the highest level of constitutional protection for free speech;**
- **promote education and parental empowerment as the most effective means to safeguard kids online;**
- **protect the ability of online service and application providers to innovate, by preserving their immunity from responsibility for content posted by others;**
- **protect the right of bloggers and other individual Americans to engage in robust political speech online without being burdened by campaign finance regulations.**

In order to preserve free speech and protect children online, the next President and Congress should take specific steps, including the following:

The next President and Congress should follow and support the Supreme Court's ruling that speech on the Internet deserves the highest level of constitutional protection.

- The Supreme Court, in striking down the Communications Decency Act ("CDA"), recognized that the Internet was different from all other electronic media such as radio and television because of its low barriers to entry, abundance of speakers, and lack of gatekeepers. The decision in the CDA case paved the way for making the Internet the innovative global medium it is today.
- The next Congress should reject legislative proposals to limit access to content online in ways that are at odds with the CDA decision.
- In the courts, the next Administration should defend the Internet's highest level of free speech protection.
- Useful links:
 - Detailed history of the court case, including text of Supreme Court Decision <http://www.cdt.org/speech/cda/>

The next President and Congress should make Internet education and parental empowerment tools the centerpiece of federal government efforts to protect children online.

- The most effective way to address child online safety concerns is through educational policies and programs for both parents and children that promote media literacy and provide practical tools that enable safe and beneficial use of the Internet.
- The next President and Congress should support funding for the development of effective educational curricula and the promotion of user empowerment tools.
- Useful links:
 - CDT analysis of Child Safety and Free Speech Issues in the 110th Congress (February 6, 2008): <http://www.cdt.org/speech/20080206freespeechincongress.pdf>
 - CDT analysis of Active Child Safety Bills Raising Free Speech Concerns Now Pending in the Senate (December 10, 2007): <http://www.cdt.org/speech/20071210FreeSpchBillsSen.pdf>
 - National Research Council report entitled "Youth, Pornography and the Internet" (2002): http://books.nap.edu/html/youth_internet/. An expert

committee headed by former Attorney General Richard Thornburg prepared this authoritative report.

- Final Report of the COPA Commission (2000):
<http://www.copacommission.org/report/>

The next President and Congress should endorse the current policy that protects Internet websites and communications intermediaries from liability for the postings of others and should oppose burdensome and ineffective technology mandates.

- The next President should oppose, and Congress should reject, proposals to require mandatory labeling of websites or Internet content in order to facilitate filtering. Mandatory content labeling is unconstitutional as a form of forced speech, it will not protect children because it cannot apply to content created and hosted overseas, and it would likely result in self-censorship of legitimate content.
- The next President should nominate to the Federal Communications Commission, and the next Congress should confirm, individuals who are strong advocates of free speech, cautious about enforcement of regulation in the broadcast arena and opposed to extending content regulation to the online world.
- The next President should oppose, and Congress should reject, proposals to require social networking websites, Internet Service Providers (ISPs), or other communications intermediaries to block access to content. The current law, which protects ISPs and other intermediaries for content created by others, has enabled service providers to host controversial but lawful speech on the Internet, creating a robust forum for ideas and discourse.
- Useful links:
 - CDT Policy Post on Section 230 protections for Internet content venues (March 31, 2008):
<http://cdt.org/publications/policyposts/2008/4>
 - CDT statement to the Senate Commerce Committee regarding protecting children on the Internet (July 24, 2007):
<http://www.cdt.org/speech/20070623child-protection.pdf>
 - Amicus brief of CDT and others to the 5th Circuit U.S. Court of Appeals on behalf of Yahoo! arguing against intermediary liability for the posting of illegal content:
<http://www.cdt.org/speech/20070705yahoobrief.pdf>

The next President and Congress should ensure that bloggers and all individual American citizens can engage in robust political speech online

without the need to comply with burdensome campaign finance limitations and reporting requirements.

- The next President should oppose, and Congress should reject, any proposals that would impose on individuals and small speakers – including bloggers – limitations on their right and ability to express their political views online, or that would require such speakers to file reports about their speech or online expenditures with the Federal Election Commission.
- The next President should nominate to the Federal Election Commission (FEC), and the next Congress should confirm, individuals who are committed to maintaining the FEC rules that exclude most online activities from the limitations and reporting requirements contained in the campaign finance laws.
- Useful links:
 - CDT/IPDI Statement of Principles for Internet Speech and Campaign Finance Regulation (May 11, 2005):
http://www.cdt.org/speech/political/principles_w_background.pdf
 - FEC Rules protecting most online political speech from campaign finance regulations (Apr. 12, 2006):
<http://www.fec.gov/law/RulemakingArchive.shtml#internet05>
 - CDT's Net Democracy Guide, aimed at helping bloggers and others understand the complex campaign finance rules:
<http://www.netdemocracyguide.org/>

▣ Protecting Consumer Privacy in the Digital Age

Americans are increasingly living their lives online and taking advantage of all the benefits that the Internet has to offer. However, consumers remain justifiably apprehensive about the privacy and security of the personal information they share with companies and divulge online. It has become more and more difficult for consumers to keep track of when, where, how, and to whom their personal information is disclosed. Meanwhile, high-tech scams involving spyware and phishing continue to increase in sophistication, undermining the trust necessary for commerce to thrive online.

Internet users need to be confident that the data they divulge to companies will be protected. At the same time, law enforcers at all levels must have the

resources they need to aggressively pursue fraudsters and malicious scammers, protect consumers, and deter future online crimes.

The next President and Congress should —

- **work together to enact comprehensive federal privacy legislation;**
- **nominate and confirm to the Federal Trade Commission individuals who will aggressively defend consumer privacy online;**
- **adequately fund the Commission to protect consumer privacy; and**
- **ensure adequate protections for personal health information.**

In order to protect consumers in the digital age, the next President and Congress should take specific steps, including the following:

The next President and Congress should work together to enact a comprehensive, technology-neutral consumer privacy law to establish meaningful safeguards for the personally identifiable information that companies collect from consumers.

- American consumers currently face a confusing patchwork of privacy standards that offer only weak protections for much personal information collected by businesses and that leave some information unprotected in some surprising ways. For example, financial privacy laws have major exceptions and, while there is a strong privacy law for video rental records, no law protects travel records or online purchasing data.
- A single, consistent privacy law would bolster consumer trust while giving both businesses and law enforcers a comprehensive standard for protecting consumers.
- The next President and Congress should work together to craft a flexible baseline privacy law to protect the personal information of American consumers both online and in the “brick and mortar” world.
- Useful links:
 - CDT/CAP Report, "Protecting Consumers Online" (July 2006)
<http://cdt.org/privacy/20060724consumer.pdf>
 - Consumer Privacy Legislative Forum Statement (June 2006)
<http://www.cdt.org/privacy/20060620cplstatement.pdf>

The next President and Congress should work together to secure adequate funding for the Federal Trade Commission, to enable it to effectively pursue its consumer protection mission, and should nominate and confirm FTC Commissioners who will make online privacy a priority.

- Consumers face an ever-increasing array of online threats, including spam, spyware, phishing, and many other types of online scams. The Federal Trade Commission is the lead federal agency for consumer protection. As the Internet evolves, the FTC's consumer protection mission is expanding and becoming increasingly complex. The Commission's jurisdiction over Internet-related issues has grown, for example, to include new laws to fight spam and identity theft. At the same time, the rapid pace of technological change, the increasing financial pay-off for malicious actors, and the transnational nature of much fraud have increased the complexity of enforcement.
- While the Internet revolution and the growth of digital technologies have heightened the FTC's importance to consumer protection, the resources available to the Commission have declined. The Commission's staff in 2008 is only 62% of the size that it was almost 30 years earlier in 1979, well before the Internet explosion.
- The next President and Congress should pledge to provide the FTC with the resources it needs to fulfill its expanded consumer protection responsibilities.
- The next President should nominate, and the next Congress should confirm, Commissioners who will protect consumer privacy. The next President should choose an FTC Chairman with a strong consumer protection focus.
- Useful links:
 - CDT Testimony on FTC reauthorization:
<http://www.cdt.org/privacy/20070912schwartz-testimony.pdf>
 - CDT Testimony on FTC appropriations:
<http://www.cdt.org/privacy/20070228schwartzftc.pdf>

The next President and Congress should develop and implement a comprehensive privacy and security framework for electronic personal health information.

- There is a broad consensus that information technology holds great promise for improving health quality, reducing errors and empowering consumers. The National Health Information Network is being built to facilitate the electronic exchange of data among health care institutions across the country. At the same time, the private sector is moving ahead with the development of online Personal Health Records.
- However, there has been little progress at the federal level in addressing the privacy and security issues associated with the growing liquidity of personally identifiable health information. The

lack of clear privacy rules threatens consumer support for health information technology. According to a 2005 study, two thirds of Americans have concerns about the privacy of their health information.

- The next President and Congress should make health information technology and health privacy an integral part of healthcare reform.
- Useful links:
 - Policy Framework for Protecting the Privacy and Security of Electronic Health Information:
<http://www.cdt.org/healthprivacy/20080514HPframe.pdf>
 - Markle Foundation Common Framework for Provider Records:
<http://www.connectingforhealth.org/commonframework/>
 - Markle Foundation Common Framework for Personal Health Records:
<http://www.connectingforhealth.oeg/phti/>
 - Collaborative response to ONCHIT RFI on NHIN:
http://www.connectingforhealth.org/resources/collaborative_response/toc.php

▣ Restoring the Balance between Security and Liberty

Privacy, one of our most fundamental rights, has been dramatically eroded in recent years as a result of the combined effect of technology changes and policy failures. Increasingly, Americans use the Internet and other digital services to access, transfer and store vast amounts of private data. Financial statements, medical records, travel itineraries, and photos of our families – once kept on paper and secure in a home or office – are now stored on networks. Electronic mail, online reading habits, business transactions, Web surfing and cell phone location data can reveal our activities, preferences and associations. At the same time, advances in technology have given the government new surveillance and data analysis capabilities. Our lives are increasingly conducted online, more and more personal information is transmitted and stored electronically, and the government’s ability to harvest, sort through, and act upon that information has increased dramatically.

However, privacy protections against unwarranted government surveillance, collection and use of personal data have failed to keep pace. Information generated by digital services is accessible to the government under weak standards based on outdated Supreme Court decisions and laws. Indeed, the major federal law on electronic communications was written in 1986, before the World Wide Web even existed.

In the wake of the 9/11 attacks, laws and policies have been adopted that unnecessarily weaken privacy rights and other constitutional liberties. The government has adopted data mining techniques, expanded electronic surveillance, and launched new identification programs without adequate safeguards for the rights of Americans. These and other programs have often been adopted before careful assessment of whether they are even likely to be effective.

Security and liberty are not mutually exclusive. The laws and investigative tools needed to protect American lives can, and must, include privacy and due process protections. Such checks and balances not only preserve liberty, but also help enhance security by ensuring that the government is focusing its limited resources on real threats and effective measures.

The next President and Congress should —

- **update electronic communications laws to account for the way that Americans communicate today;**
- **restore checks and balances on government surveillance, including vigorous judicial and congressional oversight of surveillance programs; and**
- **revisit the REAL ID Act and ensure that governmental identification programs include proper privacy and security protections.**

In order to restore the balance between security and freedom, the next President and Congress should take specific steps, including the following:

The next President and Congress should work together to enact legislation to update communications privacy laws to account for dramatic advances in technology.

- The Electronic Communications Privacy Act (ECPA) sets the standards for government surveillance of email and other communications in criminal cases. Adopted in 1986, ECPA has been outpaced by technology developments. For example, though cell phones can be used to track a person's location, ECPA does not specify a standard for law enforcement access to location information. E-mail, personal calendars, photos, and address books, which used to reside on personal computers under strong legal protections, now are stored on communications networks where privacy rules are weak or unclear.

- The next President and Congress should work together to enact legislation updating ECPA to strengthen protections against unwarranted government access to personal information.
- Useful links:
 - CDT Report on digital search and seizure: <http://www.cdt.org/publications/digital-search-and-seizure.pdf>
 - CDT Policy Post on how digital technology requires stronger privacy laws: <http://www.cdt.org/publications/policyposts/2006/4>

The next President and Congress should ensure that foreign intelligence surveillance is conducted only in full compliance with the Foreign Intelligence Surveillance Act and with appropriate checks and balances to prevent abuse.

- While ECPA governs surveillance for criminal purposes, sound and timely intelligence is also needed to head off terrorist attacks and otherwise to protect the national security. Recent history shows that intelligence gathering powers can be abused. Strong statutory standards, judicial checks and balances, and congressional oversight are critical to protect the rights of Americans and ensure that the intelligence agencies are acting effectively and within the law.
- The next President should refrain from claiming inherent authority to conduct warrantless surveillance in the U.S. and should affirm that all electronic surveillance conducted in the U.S. for intelligence purposes will conform to the Foreign Intelligence Surveillance Act, which requires a court order when a person in the U.S. is a target of surveillance.
- Legislation relating to the provisions of the PATRIOT Act that expire in 2009 should include measures to restore checks and balances on government surveillance.
- The next President should cooperate with congressional and Inspectors General oversight of intelligence surveillance, starting with a promise to enable and support oversight investigations of warrantless surveillance conducted after 9/11, and the next Congress should conduct vigorous, non-partisan oversight of the full range of intelligence surveillance programs affecting the rights of Americans.
- Useful links:
 - CDT Policy Post on pending FISA legislation: <http://www.cdt.org/publications/policyposts/2007/13>
 - CDT Testimony before the Senate Judiciary Committee and the House Intelligence Committee on proposed changes to FISA:

<http://www.cdt.org/security/20070925dempsey-testimony.pdf>
<http://www.cdt.org/security/20070918dempsey-testimony.pdf>

The next President should curtail the use of National Security Letters, and the next Congress should adopt legislation to ensure that NSLs are limited in scope and, in cases seeking sensitive records, issued with judicial approval.

- A National Security Letter is a demand by the FBI, issued without prior judicial approval, for sensitive bank, credit and communications records from financial institutions, credit reporting agencies, telephone companies, Internet Service Providers, and others. These records are important to national security investigations, but the PATRIOT Act dramatically expanded the scope of these demands while reducing the standards for their issuance. The Inspector General of the Department of Justice has found widespread errors and violations in the FBI's use of NSLs.
- To protect Americans' privacy and focus investigative resources more effectively, the next President should propose, and the next Congress should enact, legislation that would require a court order for access to sensitive personal records.
- Useful links:
 - CDT Policy Post on National Security Letters: <http://cdt.org/publications/policyposts/2007/5>
 - CDT Testimony on National Security Letters: http://cdt.org/testimony/20080421_nsl_testimony.pdf
 - DOJ Inspector General Report on NSL abuses: <http://www.usdoj.gov/oig/special/s0703b/final.pdf>

The next President and Congress should adopt a balanced framework for information sharing and analysis for counterterrorism purposes.

- Government watch lists, fusion centers, databases, and data mining programs are growing at an alarming pace without adequate safeguards.
- Connecting the dots is crucial to preventing the next attack, but inaccurate information and flawed analytic techniques can result in a person being wrongfully treated as a terrorist, with devastating consequences such as arrest, deportation, job loss, discrimination, damage to reputation, and more intrusive investigation.
- The next President should review all information sharing and analysis programs for effectiveness. The next President and Congress

should bring all information sharing and analysis programs under a framework of privacy protection, due process and accountability.

- Useful links:
 - CDT Testimony on government data mining programs: <http://www.cdt.org/testimony/20070109harris.pdf>
 - CDT Memorandum on government mining of commercial data: <http://www.cdt.org/security/usapatriot/030528cdt.pdf>
 - Markle Foundation task force report on implementing a trusted information sharing environment to prevent terrorism http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php#report1
 - GAO Report on federal data mining as of May 2004: <http://www.gao.gov/new.items/d04548.pdf>

The next President and Congress should revisit the REAL ID Act and ensure that all governmental identification programs are necessary and effective and subject to adequate privacy and security protections.

- In recent years, the federal government has launched a variety of ID card programs, including most notably the REAL ID. Some of these programs would incorporate biometric and Radio Frequency Identification (RFID) technology without safeguarding the privacy and security of information on the cards or limiting how they can be used by government or commercial entities to track the movements of ordinary Americans. Poorly designed programs could actually contribute to ID theft. The REAL ID program is already showing signs of “mission creep.”
- The next President and Congress should revisit the REAL ID program. If such review justifies continuation of the program, the next President should amend the REAL ID regulations to adequately protect privacy. If necessary, Congress should amend the REAL ID Act. The next Congress should amend the Driver’s Privacy Protection Act to further protect privacy against both governmental and commercial abuse.
- Useful links:
 - Testimony of CDT on the REAL ID Act and proposed regulations: (March 21, 2007): <http://www.cdt.org/testimony/20070321dhstestimony.pdf>
 - CDT analysis of final REAL ID regulations, with recommendations for Congress (Feb. 1, 2008): http://www.cdt.org/security/identity/20080201_REAL%20ID_hillbrief.pdf

- CDT testimony on implementation of REAL ID and Western Hemisphere Travel Initiative (April 29, 2008): <http://www.cdt.org/testimony/20080429scope-written.pdf>
- CDT comments to the Department of Homeland Security on proposed regulations to implement the REAL ID Act (May 8, 2007): <http://www.cdt.org/security/20070508realid-comments.pdf>
- CDT comments on proposed PASS Card for border crossing (Jan. 7, 2007): <http://cdt.org/security/20070108passcard.pdf>

The next President and Congress should work together to update the Privacy Act; the next President should assiduously enforce the Act's protections and those afforded by the E-Government Act of 2002.

- The Privacy Act of 1974 – the main federal law that protects the privacy of personally identifiable information in records maintained by the federal government – is seriously out of date.
- Designed for the mainframe world of 1974, the Privacy Act needs to be updated to reflect the distributed nature of government information systems and the ease with which data maintained by the government or obtained from the commercial sector can be shared and mined.
- The next Congress should adopt legislation to update and strengthen the Privacy Act, including by adopting standards for government use of commercial data. The next President should use Privacy Act exceptions sparingly.
- The next President should appoint a senior White House official as Chief Privacy Officer, to be an advocate for privacy within the Executive Branch. The Chief Privacy Officer should have a Chief Privacy Officer Council that would consist of the Chief Privacy Officers of each agency united in a structure similar to that of the Chief Information Officer Council.
- The next Administration should consistently use Privacy Impact Assessments to evaluate and address privacy risks before launching any new systems or programs collecting or processing personal data, and should issue best practices for use of Privacy Impact Assessments.
- The President should require federal agencies to increase the quality of their PIAs, require regular audits of the largest and most sensitive databases with large amounts of sensitive personal information and establish best practices and standards.
- Useful links:

- Testimony of CDT on privacy of passport files (July 10, 2008): <http://www.cdt.org/testimony/20080710schwartz.pdf>
- Testimony of CDT on new policies and laws needed to protect personally identifiable information (June 18, 2008) <http://cdt.org/testimony/20080618schwartz.pdf>
- Testimony of CDT on privacy (April 13, 2005) <http://www.cdt.org/testimony/20050413dempsey.pdf>
- GAO report on need to enhance protections for personally identifiable information in government records <http://www.gao.gov/new.items/d08795t.pdf>

▣ Promoting Global Internet Freedom

In the past decade, the Internet has been transformed from a U.S.- and western-centric network into a global medium that supports economic growth, the free exchange of ideas and democratic reforms. Internet users — even in the most repressive countries — have access to a broad range of information and ideas that challenge government propaganda. Human rights abuses can be documented and shared globally in real time. Bloggers, cyber-dissidents and other citizen media voices online are providing greater scrutiny of government conduct and demanding greater transparency. Human rights campaigns around the world can be organized quickly and inexpensively.

The global Internet's inherent openness and lack of central control is particularly threatening to authoritarian countries and those with weak rule of law and poor human rights records, such as China, Iran, Saudi Arabia, Vietnam. These countries welcome the Internet's power to fuel economic growth, but they want to harness that power while limiting the personal freedoms that the medium bestows. Many of these countries are aggressively working to remake the Internet into a tool of government control, broadly filtering out unwanted content, censoring blogs, surveiling cyber dissidents and building the capacity to closely monitor online activities. In the last five years, the number of countries engaged in state-sponsored Internet filtering has increased from a handful to two dozen.

The next President and Congress should —

- **promote Internet global freedom using all tools at the government's disposal; and**
- **insist that U.S. Internet companies adopt and adhere to a strong set of global human rights principles.**

In order to promote global Internet freedom, the next President and Congress should take specific steps, including the following:

The next President should actively promote global Internet freedom using all the available tools of trade, aid and diplomacy.

- Many countries look to the U.S. for leadership on Internet policy. When the U.S. government, either through legislation or executive action, impinges on online free speech or lowers or evades standards and procedures for surveillance, it undermines efforts to improve Internet freedom around the world. U.S. Internet policy must set a standard for the world with respect to protection of civil liberties.
- The United States government should promote global Internet freedom in unilateral negotiations and multilateral forums. The next President should make Internet freedom an explicit part of international trade and foreign aid policies, pushing nations seeking favorable trade deals or U.S. financial assistance to adopt sound Internet policies.
- Useful links:
 - CDT's testimony on Global Internet Freedom: Corporate Responsibility and the Law:
<http://cdt.org/testimony/20080520harris.pdf>

The next President should urge U.S. Internet companies to adopt and adhere to a strong set of global human rights principles.

- U.S. Internet companies are increasingly faced with government demands to assist with censorship and to turn over personal information about users, putting free expression, privacy and liberty at risk.
- Rights groups and the U.S. Congress have harshly criticized Internet companies for limiting online expression and privacy in response to government requests in China and elsewhere. Legislation is pending in Congress to prohibit U.S. companies from complying with government demands and laws that are contrary to international human rights.
- While there is significant disagreement about whether legislation is the right remedy, there is widespread agreement that Internet companies need a set of global principles to guide them when faced with laws, policies and practices that compromise free expression and privacy worldwide.
- Useful links:

- OpenNet Initiative’s research on global Internet censorship: <http://opennet.net/research>
- CDT-BSR Press Statement on multi-stakeholder initiative to draft human rights principles for the Internet industry (January 2007): <http://www.cdt.org/press/20070118press-humanrights.php>
- State Department’s Global Internet Freedom Task Force: <http://www.state.gov/g/drl/rls/78340.htm>
- Millennium Challenge Corporation’s “Guide to the MCC Indicators and the Selection Process” (Fiscal Year 2008): <http://www.mcc.gov/documents/mcc-fy08-guidetoindicatorsandtheselectionprocess.pdf>

▣ Keeping the Internet Open to Innovation

In its relatively short history, the Internet has fostered an unprecedented wave of innovation. New technologies, services and businesses have risen from scratch to transform the ways people communicate, transact business, and participate in democratic society. This remarkable growth is a direct consequence of a legal and technical framework that emphasized openness, innovation and competition. This framework has ensured that anyone with a good idea could create a new service or application and offer it to a worldwide audience, at relatively low cost and without needing permission from network operators or governments. There have been no centralized “gatekeepers” for the Internet, dictating which new services and technologies will be allowed or how they must be designed. This fundamental openness has helped generate the Internet’s success.

The future of the open Internet is not at all certain. Some network operators have suggested that they may seek to charge fees to deliver or prioritize selected traffic; some have sought to limit traffic associated with certain high bandwidth applications. This creates a risk that network operators could determine which online services will work smoothly and which will not.

Meanwhile, advocates and policymakers pursuing various legitimate policy goals — for example, protecting against copyright infringement, ensuring convenient intercept access for law enforcement, or promoting a robust 911 system — have sought to burden network operators with design mandates that could stifle innovation. In addition to design mandates, in the copyright field there are open legal questions about the extent to which those who build devices or online services should be liable for infringement committed by users. Imposing liability on true bad actors is important for enforcing copyright, but

broader or uncertain liability could create crippling liability risks for innovators and curtail the development and availability of technologies that capitalize on the Internet's strengths for interactivity, collaboration, and user-generated content.

The current environment also presents opportunities for expanding the Internet's innovative potential. Increases in bandwidth, more ubiquitous and mobile connectivity, and higher broadband penetration rates are likely to foster a wide range of new possibilities for Internet use. But in recent years, the United States has been slow to match other nation's gains in broadband penetration and speeds. Countries such as Korea and Japan have made deployment a top priority and have achieved much wider availability of broadband at much higher speeds. Wireless technologies are also likely to be at the center of many cutting edge developments, but will depend on smart and forward-thinking spectrum policy.

The next President and Congress should —

- **support policies that will keep the Internet open, innovative and free from discrimination;**
- **oppose government technology mandates that will interfere with privacy, innovation or competition;**
- **promote balanced approaches to digital copyright policy that respect both the rights of creators and the critical public interest in preserving interactivity, innovation, and free expression in the new digital media;**
- **adopt a national policy aimed at making broadband Internet access available more widely and at world-class speeds; and**
- **pursue spectrum allocation policies that permit and encourage the development of effective new ways to deliver Internet connectivity on a wireless basis.**

In order to keep the Internet open to innovation, the next President and Congress should take specific steps, including the following:

The next President and Congress should support sensible and workable safeguards that will preserve the core attributes of openness, neutrality and freedom to innovate and prevent harmful discrimination, in a manner that is compatible with the public interest in infrastructure investment and the needs for sound network management.

- Broadband providers need to be able to take steps to combat spam and other harmful traffic. However, if they start trying to play favorites among legitimate Internet traffic, it could seriously

undermine the Internet's traditional openness and neutrality; independent innovation could suffer as cooperating with broadband providers becomes a prerequisite to online success.

- The next President and Congress should work out basic rules of the road to address harmful discrimination, including measures to promote more transparency by Internet carriers, which could provide an important safeguard against practices that run contrary to the Internet's open and decentralized character. Such rules would have to be carefully crafted so they do not impose costly new burdens on network operators or involve extensive regulation.
- The next President should oppose, and the next Congress should reject, any legislation that would grant any agency or department excessive authority over Internet access.
- Useful links:
 - CDT Policy Post on network management: <http://www.cdt.org/publications/policyposts/2008/7>
 - CDT Policy Post on Internet neutrality: <http://www.cdt.org/publications/policyposts/2006/12>
 - CDT comments to Federal Trade Commission submitted in connection with Broadband Connectivity Competition Workshop: <http://www.cdt.org/speech/net-neutrality/200702028ftcneutrality.pdf>

The next President should nominate, and the next Congress should confirm, officials to the FCC, FTC, Justice Department, and Commerce Department's NTIA who are sensitive to the unique benefits of the open Internet and who oppose government technology mandates.

- Government officials need to be wary of policies that stifle innovation. Government technology design mandates are likely to be inflexible, can quickly become outdated, and can discourage innovation.
- Fighting copyright infringement is important, but the government should not mandate the inclusion of special copyright protection features in legitimate digital technologies.
- Law enforcement officials already have both the legal authority and the technical capability to wiretap Internet communications. FCC regulators should not, in an effort to make it even easier to intercept communications, impose technical mandates on innovative technologies.
- Similarly, the laudable goal of promoting a robust e911 emergency system should not justify the imposition of mandates that would prevent the creation and deployment of new technologies.

- Useful links:
 - CDT Policy Post on possible FCC wiretap and e911 technology mandates that would threaten innovation and privacy: <http://www.cdt.org/publications/policyposts/2007/12>
 - CDT Policy Post on proposal for “broadcast flag” technology mandate: <http://www.cdt.org/publications/policyposts/2005/22>

The next President and Congress should support new copyright legislation, treaties, or policies only if they protect and promote innovation and emerging forms of free expression in the digital realm.

- Current copyright law provides creators with a strong set of rights and powerful enforcement tools against infringement.
- At the same time, limitations to copyright, including “fair use,” have provided crucial breathing room for innovation and free expression.
- Efforts to reform or improve copyright law must seek to promote balance, not just expand the scope of copyright rights or remedies.
- Unbalanced proposals – like WIPO’s draft treaty to grant new rights to broadcasters or legislation that would increase the threat of damages facing makers of legitimate multi-purpose devices or services – would create new barriers to innovation and free expression.
- Useful links:
 - CDT Policy Post proposing balanced framework for online copyright protection: <http://www.cdt.org/publications/policyposts/2005/14>
 - CDT Policy Post on concerns with proposed WIPO Broadcast Treaty: <http://www.cdt.org/publications/policyposts/2006/16>
 - CDT Policy Post on “Grokster” secondary liability ruling: <http://www.cdt.org/publications/policyposts/2005/17>

The next President and Congress should develop a comprehensive strategy for fostering the expansion and improvement of the nation's broadband infrastructure.

- Government should work to gather reliable data about what the obstacles may be to expanded broadband deployment and take concrete steps to address those obstacles.
- In rural and other locations where competition is unlikely to ensure that communities are being adequately served, there may be an important role for government financial support via grants or direct municipal investment in fiber infrastructure.

- Tax incentives, questions of regulatory structure, and all other policy options should be on the table. Strategies employed by other countries warrant careful attention and consideration.

The next President and Congress should establish that fostering expanded innovation, capabilities, and consumer choice in wireless Internet connectivity will be a core goal of spectrum allocation policy.

- The next President should appoint officials to the FCC and NTIA who recognize the potential of spectrum reform and will aggressively explore opportunities for more efficient spectrum usage, including unlicensed and spectrum-sharing approaches.
- New technologies like "smart" radios may offer more efficient and dynamic ways of allocating spectrum and protecting against interference than traditional spectrum policies.
- Any interests incumbent spectrum holders may have in preserving the status quo, or that the Federal Government may have in maintaining scarcity to maximize auction revenues, should not be allowed to trump or indefinitely postpone the public benefits that may be gained by unleashing more spectrum for productive use.

▣ Promoting Open Government

The Internet has made it easier than ever before for ordinary citizens to interact with government agencies, obtain important documents and keep track of what their elected officials are doing on their behalf. The E-Government Act of 2002 encourages federal agencies to make key information available on the Internet. Unfortunately, there is a great deal of variance in terms of how well agencies have taken advantage of the digital tools at their disposal. As Americans increasingly manage their business, personal, and financial affairs electronically, they rightfully expect their government to make services and information available over the Internet.

Americans also expect their government to faithfully implement the Freedom of Information Act with timely and thorough responses to requests for information. The Clinton Administration had instructed agencies responding to requests under FOIA to release documents whenever they could. However, in 2001, the Bush Administration reversed this policy by encouraging agencies to withhold information whenever they could. The next President should fully implement the FOIA including the Open Government Act of 2007 and should re-establish a policy that favors openness.

The next President should —

- **lead an administration dedicated to transparency and accountability; and**
- **implement the Freedom of Information Act in a spirit of responsiveness and openness.**

The next President and Congress should utilize new technology to make information more readily available online and to promote citizen involvement in government decision-making.

In order to promote open government, the next President and Congress should take specific steps, including the following:

The next President should lead an administration dedicated to transparency and accountability.

- The next President should ensure that transparency and the publication of information are recognized as important goals throughout the federal government. A President can show dedication to this cause immediately upon taking office, by instructing agencies that the government’s first responsibility is to share information with the public unless a FOIA exception clearly applies.

The next President and Congress should utilize new technology to promote interactive citizen involvement in government decision-making.

- The next President and Congress should embrace Web 2.0 technology by taking advantage of wikis and social networking tools for public decision-making processes, augmenting traditional technologies and methods for commenting on proposed federal regulations and other policy initiatives.
- Agencies should ensure that all of their online resources are made available in open formats and are searchable by major public search engines.

The next President should assiduously enforce the open government laws and ensure that the executive branch is promptly and fully responsive to FOIA requests.

- The Open Government Act of 2007 creates new fiscal incentives for governmental agencies to comply with statutory deadlines for responding to FOIA requests. It enhances the ability of the public to

pursue FOIA requests by clarifying the circumstances in which an agency must pay attorney's fees in FOIA litigation. It also creates a system for tracking pending FOIA requests and it ensures that independent journalists have equal access to information available under FOIA.

- The next President should make implementation of the Open Government Act of 2007 a priority, including by ensuring that agencies will reply to FOIA requests in a timely fashion.
- Useful links:
 - CDT report "Hiding in Plain Sight," co-authored with OMBWatch. This report reveals that vast amounts of government information remain invisible when using popular search engines:
<http://www.cdt.org/righttoknow/search/>
 - CDT's "OpenCRS" project makes Congressional Research Service reports easily accessible for the public:
<http://www.cdt.org/headlines/1001>



FOR MORE INFORMATION

Please contact: Brock Meeks, CDT Director of Communications
202-637-9800

What Every Candidate Needs to Know About the Internet

May 2008 – Version 1.0

The Internet today is a technology of freedom and innovation. In less than two decades it has become a powerful, global platform for commerce, human development and democratic participation. This growth did not happen in a legal vacuum. From the outset, the Internet has been enabled by a policy framework suited to its unique technical architecture. Misguided policies could just as easily stifle the Internet's continued expansion. Increasingly, despite the Internet's success, the policy principles that supported its growth are being challenged.

The successful policy framework for the Internet emphasized openness, competition, innovation, consumer choice, and freedom of expression. For example, while ISPs themselves were relatively unregulated, they benefited from an open platform that was based on telecommunications policies of interconnection and non-discrimination. Early on, the Supreme Court ruled that the Internet was entitled to the strongest form of First Amendment free speech protection. Congress expressly decided that Web hosting services and ISPs should not be liable for the content created by others. Recognizing the importance of privacy, in 1986 Congress updated laws on government surveillance to require court orders for access to data communications, just as they had been required for telephone taps.

In recent years, policymakers seem to have forgotten what makes the Internet special. Increasingly, policy proposals treat the Internet as a problem to be solved rather than a valuable resource that must be supported. Debates over objectionable content online, protecting intellectual property, preventing terrorism, or restructuring telecommunications policy seem to have lost sight of the Internet's history and its architecture. We are seeing an increasing number of heavy-handed policy proposals that place the Internet's core characteristics at risk. Standing alone or in conjunction with marketplace and technological changes, these policies could fundamentally alter the very elements of the Internet that have made it so successful.

▣ Key Features of the Internet

These are the key features of the Internet that have been largely responsible for its success — and can continue to do so, as long as they are enabled by a sound policy framework:

USER EMPOWERMENT

The Internet is uniquely user-controlled. To a far greater extent than users of any other electronic medium, Internet users have the power to choose where they will go online and what they will see or hear. Users can configure their browsers and their search engines to avoid content they consider objectionable. They can install filters to block unwanted content and email. Assuming users are provided with notice and genuine choices, they can decide what software to download. They can install security software to protect against many forms of fraudulent behavior. Empowering users — especially parents, librarians and educators to use technology tools to shield children from inappropriate content is far more effective than any government censorship regime. Efforts to address Internet challenges should focus first on policies that empower users, rather than empowering the government or requiring intermediaries to exert control.

OPEN, DECENTRALIZED, INTEROPERABLE, NO GATEKEEPERS

The Internet is, by design, decentralized. Its power is at the edges of the network, unlike previous mass media. The brilliance of its underlying technology is that any device can be attached to the network and interoperate with another device, with little regard for physical distance. The decentralized architecture of the Internet means there are few chokepoints. Censorship is difficult at the core of the Internet because network operators and ISPs simply did not build a lot intelligence into their networks; the sheer quantity of traffic precludes effective control from one point to another. Network operators focus on speed, on getting Internet traffic to its intended destination, without pausing to examine every electronic bit for compliance with standards of acceptability.

If ISPs, Web hosts, and Web site creators become liable for content posted by others, the Internet would be stifled by gatekeepers and it would cease to be a medium where everyone has an opportunity to make their voices heard. Increasingly, policymakers have been seeking to turn service providers into policemen, forcing ISPs to filter undesirable content and refuse access to undesirable users. Policymakers have also sought to delegate enforcement obligations to other components of online commerce, notably credit card companies, forcing them to block certain payments for undesirable services or content.

NON-DISCRIMINATION

Early policy choices confirmed and enforced the Internet's open platform. In the dial-up world of the Internet's emergence, the network's edge architecture was supported by telecommunications policies that required network operators to allow any equipment to be attached to their networks and to carry all traffic on a non-discriminatory basis. Innovators did not need to negotiate with network operators to connect a modem to the network or to make their content and services available to a wide audience. This allowed innovation on the Internet to flourish. On the converged broadband Internet, there is a risk that network gatekeepers could engage in discrimination, favoring some content, or some uses, over others, in a way that diminishes innovation and erects barriers to new voices. It is essential that the core elements of these open and non-discriminatory principles are applied to the converged broadband Internet. Doing so poses difficult challenges, but must be achieved.

INNOVATION, NOT TECHNOLOGY MANDATES

The Internet's simple core supports a remarkable degree of innovation. It does so on the basis of voluntary technical standards. Even though the Internet was "born" under the auspices of the Pentagon, the U.S. government never mandated its core technologies. Those technologies were developed by scientists and broadly adopted because they worked. From the outset, Internet policy was based on the notion that the government should not design technology; in order to ensure innovation, that function was best left to the marketplace. For example, early efforts to control encryption were abandoned, in part because of the recognition that government-mandated back doors would undermine security, rather than improve it.

Increasingly, policymakers have been asserting control over the Internet's technology and imposing design mandates on Internet services and applications. The FCC has already imposed on the Internet design mandates for wiretapping. Proposals abound to do the same to protect intellectual property, and consideration of such mandates is likely to continue growing. Such mandates pose a severe threat to innovation.

ABUNDANCE AND LOW BARRIERS TO ENTRY

Traditional radio and television technology was bound by a limited technical capacity to exploit the electromagnetic spectrum. Consequently, regulation of the airwaves was deemed necessary in order to allocate what was seen as a scarce resource. The Internet by contrast can accommodate an essentially unlimited number of points of entry and an essentially unlimited number of speakers. Its open platform accommodates many-to-many, one-to-many and one-to-one communication. Compared to the cost of a printing press, a TV

station or a radio tower, the cost of launching a Web site is remarkably low — and that Web site can reach the entire world.

Low barriers to entry and participation have led to a relative equality of voice and a democratization of expression. In terms of free speech, an environmental activist can reach the same people as an oil company. A blogger can impact an election as much as a major newspaper. And a new content or application provider can emerge from nowhere to become an extraordinary success with relatively low investment and without having to obtain a government license or negotiate with an incumbent to offer new services.

GLOBAL

While the digital divide in the developing world poses serious challenges, the Internet from its inception was a global medium. This greatly limits the reach and effectiveness of many national regulatory efforts, especially those directed at controlling content. Given the global nature of markets, burdensome regulation in the U.S. could send innovation overseas.

Comments to CDT's Internet in Transition: Election 2008

As of November 4th, 2008

JUNE 4, 2008 FROM PETER SWIRE IN CONSUMER PRIVACY

HIPAA should be updated so that key organizations are covered by federal privacy protections. For instance, many "regional health information organizations" (RHIOs) gather data from many providers, but are not themselves covered by HIPAA. Congress should move forward with legislation that covers the health-related entities that are most important to the future of how medical records are actually handled.

JUNE 4, 2008 FROM PETER SWIRE IN OPEN GOVERNMENT

The Justice Department should clearly return to the FOIA policies under Janet Reno, rather than the overly restrictive approach of recent years.

The Congress can do better as well. Committees and subcommittees in the Congress should do a much better job of recording votes in markups and letting the public have access to other information at the point where decisions are often made -- in committee.

JUNE 5, 2008 FROM CHRIS HANKIN IN OPEN GOVERNMENT

This section misses the most important point: that the internet and electronic media can and should be utilized more effectively to enable timely, useful, and interactive access to government services and programs, while also ensuring that no US persons are unfairly discriminated against. Such discrimination shall include issues with regard to accessibility by persons with disabilities, by individuals and entities with limited financial means, and by small business. Important to accomplishing this will be greater government use of open standards, open source, and open formats.

JUNE 6, 2008 FROM DAVID SOBEL IN OPEN GOVERNMENT

The most persistent, systemic problem in FOIA compliance is a lack of agency resources devoted to the FOIA process. Agencies prefer to devote resources to disseminating the information *they* want to disclose, rather than the information the *public* wants to obtain. Both the President and Congress must commit to providing specific, dedicated appropriations to agencies to fully comply with their

FOIA obligations. Only then will agencies no longer have the "lack of resources" excuse to justify the persistent processing delays that require requesters to wait months (and often years) to receive responses to FOIA requests.

JUNE 9, 2008 FROM BOB GELLMAN IN CONSUMER PRIVACY

We need more privacy leadership than the FTC or any other existing agency can provide. Overall, consumers need better protection than the FTC provides and not just for privacy. There are so many areas where consumers are ripped off by fraudulent and scummy business practices, and the FTC can't even pretend to keep up. It is okay, if you like, to try to improve the FTC. I would rather look for alternatives for consumer protection. But for privacy, we need a genuine, single purpose, and INDEPENDENT privacy policy agency. Among many other things, a privacy policy agency will help to keep the FTC from compromising consumer privacy rights as it has done too often in the past. A privacy policy agency will also provide expertise to the Congress (so it doesn't have to reinvent the wheel for every privacy bill under consideration). An independent agency will keep pressure on OMB and other executive agencies to do the right thing. It will provide leadership for privacy officers in federal agencies. It will assist businesses to meet reasonable consumer privacy needs. Just about every other major country has some type of independent national privacy agency. We need one too. It does not need regulatory authority to be useful, and I do not suggest that it should have any regulatory powers. A soapbox will do nicely.

JUNE 9, 2008 FROM BOB GELLMAN IN OPEN GOVERNMENT

I agree with David Sobel about resources, but dedicated appropriations for FOIA will kill the law. In year one, an agency gets a FOIA line item. In year two, it asks for the line item to be cut or eliminated. Why would any agency fight for FOIA funds instead of its own organic programs? The Appropriations Committees don't much care about FOIA. They will take FOIA line item funds and use them for their pet programs. In the end, the agency will say that it didn't get an appropriation for FOIA so it doesn't have to comply with the law. The courts will uphold that conclusion. Game over. The resource game is, unfortunately, a loser for FOIA advocates. We need substantive changes to FOIA. We need to provide that more White House offices are covered by the law. It should cover the Smithsonian, GAO, CBO, and the Library of Congress. It should NOT cover the Congress itself. We also need to narrow and clarify exemptions, although reaching consensus on that front won't be easy. Having the Attorney General issue pro-FOIA memos will do nothing meaningful. It didn't change anything when Janet Reno did it. It only has symbolic value, and we need more substance and not just symbols. As for the Justice Department, we should take away its FOIA oversight authority. You can't ask the same agency to both encourage compliance while they defend agency withholding.

SEPTEMBER 14, 2008 FROM DANIEL IN FREE SPEECH

Theres no dout, there should be limits to the avalibility of inappropriate material on the internet,how easy does it get..To shock and awe..Do we have no shame?

OCTOBER 2, 2008 FROM JOHN IN FREE SPEECH

The government has no rights or authority over the internet. Show me in the constitution where the people gave the govt anything other than free speech.

Parents, take your children off the internet. They really don't belong here anyway. If they get in here, it's the same as sneaking into the adults library.

This isn't sesame street, and keep them out of restuarants and casino's as well, I'm not gonna modify my habits to fit your family, and this ain't McDonalds either.

OCTOBER 2, 2008 FROM JOHN IN FREE SPEECH

The govt has no authority over the internet, in any way shape or mean, no constitutional authority exists for them to even discuss the internet.

the govt has the constitution mandate to secure our borders and ports, and until they do that, they have no business even talking about another issue, and that includes, the friggin internet. As far as the rest of the provacy concerns, if the comany is stupid enough to connect it's servers to the internet, then you have just brought your database to my front room, and when I get bored enough, I might take on your front door, so if I were you, and to avoid the mega million dollar lawsuits, you would lock up your internal servers and protect them in the same file room you used to use for your paper files or suffer the consequences. And the first one of you that lose my persoanl data, for any reason, (I don't care if the guard died... you should have had two.)

I will sue you until you need a bailout.