# UNITED STATES OF AMERICA

| | 2009 | 2011 |
|---|---|---|
| **INTERNET FREEDOM STATUS** | **n/a** | **Free** |
| **Obstacles to Access** | n/a | 4 |
| **Limits on Content** | n/a | 2 |
| **Violations of User Rights** | n/a | 7 |
| **Total** | **n/a** | **13** |

**POPULATION:** 309.6 million
**INTERNET PENETRATION:** 78 percent
**WEB 2.0 APPLICATIONS BLOCKED:** No
**SUBSTANTIAL POLITICAL CENSORSHIP:** No
**BLOGGERS/ONLINE USERS ARRESTED:** No
**PRESS FREEDOM STATUS:** Free

## INTRODUCTION

Access to the internet in the United States remains quite free compared with the rest of the world. Users face few restrictions on their ability to access and publish content online. The courts have consistently held that federal and state constitutional prohibitions against government regulation of speech apply to material published on the internet. In addition, statutory immunity for online service providers continues to play an important role in fostering business models that permit open discourse and the free exchange of information.

However, several developments in recent years have placed the government and internet freedom advocates at odds over aspects of internet regulation as well as issues surrounding online surveillance and privacy. The United States lags behind many major industrialized countries in terms of broadband penetration, and the strength and legal viability of recent rules concerning network neutrality remain uncertain. The current administration appears committed to maintaining broad surveillance powers with the aim of combating terrorism, child pornography, and other criminal activity, and it has been reported that the government is seeking expanded authority to control the design of internet services to ensure that communications can be intercepted when necessary.

## OBSTACLES TO ACCESS

Access to the internet in the United States is largely unregulated. It is controlled in practice by a small group of cable television and telephone companies that own and manage the

network infrastructure. This model has come into question in recent years amid growing concern that it is adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[1] Observers have warned that if recent "network neutrality" regulations—discussed in greater detail below—prove too weak or are rejected by Congress or the courts, the dominant companies may decide not to continue to carry internet traffic in a content-neutral fashion.

Although the United States is one of the most connected countries in the world, it has fallen behind many other developed countries in terms of internet speed, cost, and broadband availability.[2] Approximately 78 percent of all Americans have access to the internet,[3] but only 66 percent of adults use high-speed broadband connections.[4] While the broadband penetration rate is considered high by global standards, it puts the United States significantly behind countries such as Japan, South Korea, Norway, and Sweden. Lack of high-speed internet access is particularly evident in rural areas, where the low population density makes it difficult to justify large investments in network infrastructure. In fact, broadband service is not yet available to 5 to 10 percent of U.S. residents, most of whom live in rural counties.[5]

African Americans, those living in rural areas, and those earning less than US$30,000 annually are the groups least likely to have access to the internet, though internet penetration among African Americans has been growing at significantly higher rates than in the general population. In a survey conducted by the Pew Research Center, when asked why they do not use the internet, many nonusers said they did not see the internet's relevance in their lives. They also cited factors such as availability, usability, and price as key deterrents. About 61 percent of nonusers said they would require assistance to go online if they chose to do so.[6]

[1] Mark Cooper, "The Socio-Economics of Digital Exclusion in America, 2010" (paper presented at 2010 TPRC: 38th Research Conference on Communications, Information, and Internet Policy, Arlington, Virginia, October 1–3, 2010).

[2] According to a study by the Organization for Economic Cooperation and Development (OECD), as of June 2010 the United States was ranked 9th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 14th, on fixed-line broadband penetration. See OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2010," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2010," http://www.oecd.org/dataoecd/21/35/39574709.xls, accessed March 4, 2011.

[3] International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," available at http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed March 4, 2011.

[4] Aaron Smith, *Home Broadband 2010* (Washington, DC: Pew Internet and American Life Project, August 11, 2010), http://www.pewinternet.org/Reports/2010/Home-Broadband-2010/Summary-of-Findings.aspx; National Telecommunications Information Administration (NTIA), *Networked Nation: Broadband in America 2008* (Washington, DC: U.S. Department of Commerce, 2009).

[5] Amy Schatz, "Want Broadband? New Maps Show Options," *Digits* (blog), *Wall Street Journal*, February 17, 2011, http://blogs.wsj.com/digits/2011/02/17/want-broadband-new-map-shows-options/.

[6] Smith, *Home Broadband 2010*.

Mobile telephones, particularly models that enable internet access, have become ubiquitous in the United States. The mobile-phone penetration rate is roughly 91 percent.[7] As of mid-2010, about 38 percent of mobile-phone users reported accessing the internet on their phones, and roughly half of those users accessed the internet on a daily basis.[8] A growing number of people use their phones to check e-mail, visit social-networking sites such as Facebook, and engage in online commerce, prompting many companies to develop special applications and versions of their websites that are designed for mobile-phone viewing.

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency of the executive branch, is charged with regulating radio and television broadcasting, all interstate communications, and all international telecommunications that originate or terminate in the United States. Although the FCC is not specifically tasked with regulating the internet or internet-service providers (ISPs), it has claimed jurisdiction over some internet-related issues, such as the recent rules regarding network neutrality. Other government agencies, such as the National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic, and technological policies and regulations. It is incumbent upon the U.S. Congress to create laws that govern the internet and delegate regulatory authority, and government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

Recognizing that internet penetration and connection speeds in the United States have been outpaced by those in several other developed countries, Congress has devoted funding to improving the broadband infrastructure and instructed the FCC to create a National Broadband Plan that will ensure broadband availability for all U.S. residents. Lawmakers required that this plan include a detailed strategy for reducing costs to consumers and maximizing the use of broadband to enhance health care delivery, energy efficiency, economic growth, education, and other public goods.[9] After issuing a notice of inquiry in April 2009 and weighing input from a wide variety of business, government, and civil society organizations,[10] the FCC issued its National Broadband Plan in March 2010. First among the goals is to provide at least 100 million U.S. homes with "affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at

[7] ITU, "ICT Statistics—Mobile Cellular Subscriptions," available at http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed March 4, 2011.
[8] Aaron Smith, *Mobile Access 2010* (Washington, DC: Pew Internet and American Life Project, July 7, 2010), http://www.pewinternet.org/Reports/2010/Mobile-Access-2010/Summary-of-Findings.aspx; Amy Gahran, "Survey: U.S. Mobile Web Access Growing Fast," CNN, July 8, 2010, http://articles.cnn.com/2010-07-08/tech/mobile.internet.access.pew_1_cell-phone-users-feature-phones-mobile-internet?_s=PM:TECH.
[9] American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. (2009).
[10] Stephanie Condon and Marguerite Reardon, "FCC Seeks Input on National Broadband Plan," CNet News, April 8, 2009, http://news.cnet.com/8301-13578_3-10214974-38.html.

least 50 megabits per second."[11] As part of the initiative, the government has started providing subsidies to ISPs that offer satellite-based internet access in rural areas.[12]

Between 3,000 and 4,000 ISPs currently operate in the United States, although 15 of them control approximately 75 percent of the market.[13] Most of the network cables and other infrastructure are owned by large telephone and cable-television companies, such as Comcast, Time Warner, AT&T, and Verizon. Until 2005, those companies were required to grant "nondiscriminatory" access to their wire networks to other ISPs to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed the network owners from the obligation to lease their lines to competing ISPs. The proponents of deregulation claimed that this step would provide more incentive for large cable and telephone companies to further develop and upgrade their networks, while opponents claimed that it would lead to fewer options for consumers, higher prices, and worse service.

One of the main policy debates surrounding the internet in the United States has to do with the concept of network neutrality, according to which network providers must treat all content, websites, and platforms equally when managing data traffic.[14] Supporters of the principle argue that without it, ISPs would be able to block certain content and applications, or give preferential treatment to some content providers for a fee. Although concerns about net neutrality began emerging in the early 2000s, the issue did not gain widespread attention until the emergence of a 2007 case involving Comcast, a cable-television company and major ISP. That year, it was revealed that the company was slowing down and blocking certain types of peer-to-peer file-sharing traffic.[15] Comcast claimed that it was forced to do so because certain high-volume users were clogging its network by repeatedly sharing large files, but its blocks were inconsistent and seemingly deceptive. For example, while engaged in peer-to-peer file sharing, a user would get a message from Comcast that looked like it came from the other computer, instructing him to stop the communication. A number of public-interest groups and academics requested that the FCC declare such blocking to be a violation of the agency's internet policy principles.[16] The FCC agreed, and Comcast appealed to the federal courts.[17] In April 2010, a federal appeals court sided with Comcast

[11] Federal Communications Commission (FCC), *National Broadband Plan: Connecting America* (Washington, DC: FCC, 2010), http://www.broadband.gov/download-plan/.

[12] Rural Utilities Service Broadband Initiatives Program, *Round Two Application Directory: Satellite, Technical Assistance, and Rural Library Broadband Grant Applications* (Washington, DC: U.S. Department of Agriculture, August 30, 2010), http://www.broadbandusa.gov/BIPportal/files/BIP_Sat_TA_RLB_App_Directory.pdf.

[13] "ISP Usage and Market Share: ISP Trends, Stats and Analysis," StatOwl.com, February 2011, http://www.statowl.com/network_isp_market_share.php.

[14] Tim Wu, "Network Neutrality FAQ," Timwu.org, http://timwu.org/network_neutrality.html, accessed March 4, 2011.

[15] Peter Svensson, "Comcast Blocks Some Internet Traffic," MSNBC, October 19, 2007, http://www.msnbc.msn.com/id/21376597/ns/technology_and_science-internet/.

[16] "Comcast Complaint," Public Knowledge, http://www.publicknowledge.org/issues/comcastcomplaint, accessed March 4, 2011.

[17] FCC, "Commission Orders Comcast to End Discriminatory Network Management Practices," news release, August 1, 2008, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

and overturned the FCC's ruling against the company. The decision, which came shortly after the release of the National Broadband Plan, also found that the FCC did not have the authority to regulate ISPs under the legal framework the agency had cited, challenging its ability to protect consumers on the internet.[18]

In December 2010, the FCC issued a compromise ruling on net neutrality that instructs fixed-line service providers not to block access to or unreasonably discriminate against lawful websites, applications, or devices. The rules for wireless broadband providers are much more limited, however, restricting only some types of blocking and saying nothing about discrimination. ISPs are allowed to offer tiered services at different prices under the new regulations.[19] FCC chairman Julius Genachowski claimed that the rules would protect "internet freedom and openness and promote robust innovation and investment."[20] Some civil society organizations expressed disappointment that the commission did not take a stronger stance on net neutrality that would have applied the Communications Act's "common carrier" provisions, though they agreed that the FCC operated in a free, fair, and independent manner.[21]

## LIMITS ON CONTENT

Access to information on the internet is generally free from government interference. There is no government-run filtering mechanism affecting content passing over the internet or the mobile-phone network. Users with opposing viewpoints engage in a vibrant online political discourse, and face almost no legal or technical restrictions on publication or access.

Although the government does not restrict any political and social content, legal rules that apply to other spheres of life have increasingly been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful content, gambling, and financial crime have presented a strong impetus for aggressive legislative and executive action.

Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988,

[18] Comcast Corporation v. Federal Communications Commission, No. 08-1291, U.S. Court of Appeals for the District of Columbia Circuit, April 6, 2010, http://www.cadc.uscourts.gov/internet/opinions.nsf/EA10373FA9C20DEA85257807005BD63F/$file/08-1291-1238302.pdf.

[19] FCC, "Report and Order: In the Matter of Preserving the Open Internet, Broadband Industry Practices," FCC 10-201, December 21, 2010, http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf.

[20] Sara Jerome, "Genachowski on Net-neutrality: "I Reject Both Extremes," *Hillicon Valley* (blog), *The Hill*, December 20, 2010, http://thehill.com/blogs/hillicon-valley/technology/134597-genachowski-on-net-neutrality-i-reject-both-extremes.

[21] "Network Neutrality," Public Knowledge, http://www.publicknowledge.org/issues/network-neutrality, accessed March 4, 2011.

all producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies can seize the domain name of an offending website after obtaining a court order.

Congress has passed several laws designed to restrict adult pornography and shield children from harmful content, such as the Child Online Protection Act of 1998 (COPA), but they were later overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedoms of speech and the press. One law that is currently in force is the Children's Internet Protection Act of 2000 (CIPA), which requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing "visual depictions that are obscene, child pornography, or harmful to minors." Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, and about one-third of public libraries in 2007 decided to forgo such financial support to avoid the filtering requirement.[22] Moreover, under the U.S. Supreme Court's interpretation of the law, adult users can request that the filtering be removed without having to provide a justification.[23]

Apart from clearly illegal content such as child pornography, the government in recent years has started more aggressively pursuing alleged infringements of intellectual-property rights on the internet. Over the past year alone, the Immigration and Customs Enforcement division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharing sites that allegedly linked to illegal copies of music and films, and sites that sell counterfeit goods.[24] In September 2010, Senator Patrick Leahy, a Democrat from Vermont, proposed a Combating Online Infringements and Counterfeits Act (COICA), which would have authorized the attorney general to suspend any domain name that provided access to websites dedicated to copyright-infringing activities. However, the bill was criticized by some internet-freedom advocates for its potential effects on political and other speech, and it was defeated before reaching the Senate floor.

The recent activities of the antisecrecy organization WikiLeaks have touched off a serious debate about the use of the internet to publicize sensitive or classified government documents. Working with a number of traditional news outlets, WikiLeaks has published several tranches of U.S. government material that was allegedly stolen and leaked by a U.S. Army intelligence analyst, Bradley Manning. This information has included a video

[22] Charles C. McClure and Paul T. Jaeger, *Public Libraries and Internet Service Roles: Measuring and Maximizing Internet Services* (Chicago: American Library Association, 2009), 42.
[23] Bob Bocher, "Children's Internet Protection Act, CIPA: A Brief FAQ on Public Library Compliance," Wisconsin Department of Public Instruction, February 2004, updated March 11, 2010, http://dpi.state.wi.us/pld/cipafaqlite.html.
[24] Corynne McSherry, "U.S. Government Seizes 82 Websites: A Glimpse at the Draconian Future of Copyright Enforcement?" Electronic Frontier Foundation, November 29, 2010, https://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future.

recording from a 2007 incident in which journalists and Iraqi civilians were killed by U.S. forces (April 2010), more than 76,900 documents on the war in Afghanistan (July 2010), almost 400,000 documents about the war in Iraq (October 2010), and reams of diplomatic cables from the U.S. State Department (November 2010).

Since the release of the diplomatic cables, the WikiLeaks website has faced some unofficial, nongovernmental actions that restricted its ability to operate and obtain financial support. In late November 2010, for example, the site was removed from the data-storage service of the online commerce company Amazon, which claimed that WikiLeaks had violated its terms of service.[25] A day later, WikiLeaks' domain-name service provider, EveryDNS, ended its relationship after suffering distributed denial-of-service (DDoS) attacks by the organization's opponents.[26] The following week, the online payment service PayPal froze the account WikiLeaks had used to receive donations from the public, claiming that the group was in violation of its terms of service.[27] While each company that severed ties with WikiLeaks claimed to be acting independently and without government influence, their decisions came amid fierce public criticism of WikiLeaks by executive branch officials and prominent members of Congress.[28] Various U.S. government agencies and officials have gone so far as to instruct federal employees without proper clearance to refrain from reading the leaked cables, since they are still regarded as classified documents. The Air Force went a step further and blocked on its internal network any sites that published the cables, including those of the *New York Times* and the *Washington Post*.[29]

Although Manning, the soldier accused of passing the classified information to WikiLeaks, is facing a military prosecution that could end with a sentence of life in prison, the government to date has not filed charges over the actual publication of the leaked material, nor has it sought to block access to the information or ban publication of future leaks.

A communications start-up community is thriving in the United States, despite the recent economic recession, and such innovators and entrepreneurs regularly offer new technological tools at no cost to the public. Popular web applications like the video-sharing site YouTube, the social-networking site Facebook, the Twitter microblogging service, and international blog-hosting services are all freely available. The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen

[25] Geoffrey A. Fowler, "Amazon Says WikiLeaks Violated Terms of Service," *Wall Street Journal*, December 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.
[26] Kevin Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities," *Wired*, December 3, 2010, http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.
[27] Kevin Poulsen, "PayPal Freezes WikiLeaks Account," *Wired*, December 4, 2010, http://www.wired.com/threatlevel/2010/12/paypal-wikileaks/.
[28] Ewen MacAskill, "WikiLeaks Website Pulled by Amazon After US Political Pressure," *Guardian*, December 2, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.
[29] Eric Schmitt, "Air Force Blocks Sites that Posted Secret Cables," *New York Times*, December 14, 2010, http://www.nytimes.com/2010/12/15/us/15wiki.html.

journalism has changed the ways in which many people receive news. Blogs and electronic media outlets reporting from various points on the political spectrum now have greater readership than most printed periodicals. Nearly all nongovernmental organizations and causes have a presence on the internet and use it for advocacy and social mobilization. E-mail campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and putting a spotlight on issues ranging from environmental degradation to hate crimes.[30]

The internet has also profoundly influenced political campaigning and fundraising. Until recently, most election campaigns relied on large donations from a limited pool of wealthy contributors. However, the success of current U.S. president Barack Obama's 2008 campaign, which was propelled by millions of small, online contributions, demonstrated the efficacy of the internet in mobilizing mass political support. Obama's election team was able to raise over half a billion dollars in internet-based donations, with an average donation of about $80.[31] In addition, the campaign's use of e-mail, social-networking tools, and online videos was watched and eventually emulated by political operatives in the United States and around the world.

## VIOLATIONS OF USER RIGHTS

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court applied established standards on those rights to the internet, and the lower courts have consistently enforced them. Two federal laws also provide significant protections for online speech: Section 230 of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) provides immunity for ISPs and online platforms such as YouTube and Facebook that carry content created by third parties, and the Digital Millennium Copyright Act (DMCA) requires copyright owners to notify intermediaries to have allegedly infringing material removed. These statutes effectively enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.

The U.S. government generally does not prosecute individuals for posting information on the internet. As of the end of December 2010, it had taken no decisive action against either WikiLeaks or its founder, Julian Assange, an Australian citizen. However, Attorney General Eric Holder has stated that his office is looking into whether

[30] See for example the Care2 "Keep Sewage Out of Our Rivers!" petition at http://www.thepetitionsite.com/takeaction/200/475/680/, and Steve Williams, "President Obama Signs Hate Crimes Bill—Thank You to the 25,000 Care2 Members That Helped It Reach His Desk!" Care2, October 28, 2009, http://www.care2.com/causes/civil-rights/blog/25-000-care2-members-help-secure-presidents-signature-on-hate-crimes-bill/.

[31] Jose Antonio Vargas, "Obama Raised Half a Billion Online," *44* (blog), *Washington Post*, November 20, 2008, http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html.

any such charges would be appropriate.[32] Many analysts argue that given the applicable laws and legal precedents, the government is unlikely to prosecute Assange or WikiLeaks for merely publishing leaked information. But some reports have suggested that federal officials are attempting to build a case that WikiLeaks played a conspiratorial role in the Army analyst's unauthorized downloading of classified documents from U.S. military computers, or in his subsequent transmission of the material to WikiLeaks.[33]

There are no legal restrictions on user anonymity on the internet, and constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[34] In June 2010, the Obama administration released plans for a National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to ensure the creation of an "identity ecosystem" in which internet users and organizations can more completely trust one another's identities and systems when carrying out online transactions.[35] While the plan does not include mandatory registration, some commentators have expressed their concerns about its potential effects on anonymous speech.[36]

The contents of internet communications are generally protected from government intrusion by constitutional rules against unreasonable searches and seizures,[37] but law enforcement and intelligence agencies can access such information with varying degrees of judicial oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can obtain court orders to monitor specified internet communications if they persuade a judge that there is probable cause to believe that a crime has been or will be committed. The Communications Assistance for Law Enforcement Act (CALEA) requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so,[38] and some in the Obama administration suggested in late 2010 that the law could be expanded to

[32] "Holder: Wikileaks Probe 'Serious Investigation,'" KTVU San Francisco, December 10, 2010, http://www.ktvu.com/news/26092558/detail.html.
[33] Charlie Savage, "U.S. Weighs Prosecution of Wikileaks Founder, but Legal Scholar Warns of Steep Hurdles," *New York Times*, December 1, 2010, http://www.nytimes.com/2010/12/02/world/02legal.html.
[34] "Apple v. Does," Electronic Frontier Foundation, http://www.eff.org/cases/apple-v-does, accessed March 4, 2011.
[35] A site created to foster discussion on the proposed strategy can be found at http://www.nstic.us/.
[36] Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" *Blog of Rights*, American Civil Liberties Union, January 7, 2011, http://www.aclu.org/blog/technology-and-liberty/dont-put-your-trust-trusted-identities; Jim Dempsey, "New Urban Myth: The Internet ID Scare," *Policy Beta* (blog), Center for Democracy and Technology, January 11, 2011, http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare.
[37] Paul Ohm, "Court Rules Email Protected by Fourth Amendment," *Paul Ohm's Blog*, *Freedom to Tinker*, December 14, 2010, http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment.
[38] The FCC does not classify Skype as an "interconnected VoIP."

permit increased access to online communications tools such as Gmail, Skype, and Facebook.[39]

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which broadly expanded the government's surveillance and investigative powers in cases involving terrorism. Among other things, the law requires ISPs to provide more detailed information about the internet activities of terrorism suspects—including their browsing history—with less judicial oversight and, in some cases, without probable cause. In February 2010, three expiring provisions of the USA PATRIOT Act were renewed for an additional year, including the government's broad authority to conduct roving wiretaps of unidentified or "John Doe" targets, to wiretap "lone wolf" suspects who have no known connections to terrorist networks, and to secretly access a wide range of private business records without warrants under Section 215.[40]

[39] Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet," *New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1.
[40] "Patriot Act Excesses," *New York Times*, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.