Freedom House

United States

	2013	2014
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	1	2
Violations of User Rights (0-40)	12	13
TOTAL* (0-100)	**17**	**19**

* 0=most free, 100=least free

Population:	312 million
Internet Penetration 2013:	84 percent
Social Media/ICT Apps Blocked:	No
Political/Social Content Blocked:	No
Bloggers/ICT Users Arrested:	No
Press Freedom 2014 Status:	Free

Key Developments: May 2013 – May 2014

- In January 2014, a federal appeals court struck down regulations on net neutrality, raising new concerns about discriminatory treatment of content (see **Obstacles to Access**).
- Self-censorship among journalists and writers reportedly increased due to an awareness of the potential threats to anonymity posed by surveillance of online communications (see **Limits on Content**).
- Revelations about NSA surveillance continued as more documents were leaked, including reports in September 2013 that the NSA had been working to undermine and circumvent online encryption tools (see **Violations of User Rights**).
- Advocates and lawmakers continued to push for legal reform of the Electronic Communications Privacy Act, which would require the government to obtain a warrant in order to compel online service providers to disclose private communications (see **Violations of User Rights**).

Introduction

Access to the internet in the United States remains relatively 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. The law also protects online service providers from liability for infractions committed by their users, a policy that fosters business models that permit open discourse and the free exchange of information.

The future of net neutrality in the United States remains uncertain, with the current discussion centered on regulatory safeguards that protect against conduct by internet service providers (ISPs) favoring some internet traffic over others. In January 2014, a court struck down the Open Internet Rules that had been adopted by the Federal Communications Commission to protect net neutrality. As a result, there are currently no legal protections for net neutrality in place. In May 2014, the FCC sought comment on a new regulation that left open the possibility of allowing content providers to strike deals with ISPs for preferential treatment, sparking significant mobilization from a range of stakeholders who urged the FCC to protect net neutrality.

Over the last year, a series of secret documents leaked to major news outlets revealed that the National Security Agency (NSA) is conducting widespread surveillance of American citizens and people around the world. Advocates and academics argue that such surveillance has a chilling effect on writers,[1] human rights activists,[2] religious minorities,[3] and ordinary citizens. Additionally, leaked documents showed that the NSA had been developing programs to crack the security of anonymizing tools such as Tor and other encryption programs.[4] Civil society groups and technology companies have lobbied for surveillance reform, and legislation is moving in Congress that includes a number of provisions to increase transparency and protect individuals' right to privacy with regard to data and online communications.[5]

Additionally, advocates and lawmakers continue to fight for reform of the Electronic Communications Privacy Act (ECPA), an outdated law that governs how government officials can access private communications through online service providers. Designed for the state of technology in 1986, the law allows for electronic mail to be obtained by the government under a standard weaker than that applicable to postal mail. ECPA reform, if passed, would require government officials to obtain a warrant before compelling online service providers to disclose private communications, including email and documents stored using cloud services.[6]

1 "NSA Drives U.S. Writers to Self-Censor," PEN America, November 11, 2013, http://www.pen.org/chilling-effects.

2 "EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association," Electronic Frontier Foundation, November 6, 2013, https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association.

3 Darwinder S. Sidhu, "The Chilling Effect of Government Surveillance on the Use of the Internet by Muslim-Americans," 7 U. Md. L.J Race Relig. Gender & Class 375 (2007), http://digitalcommons.law.umaryland.edu/rrgc/vol7/iss2/10.

4 Barton Gellman, Craig Timberg, and Steven Rich, "Secret NSA documents show campaign against Tor encrypted network," *Washington Post*, October 4, 2013, http://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.

5 The USA Freedom Act (H.R. 3361/S. 1599), Govtrack.us, https://www.govtrack.us/congress/bills/113/hr3361. See also: Brandon Moss, Amie Stepanovich, "One step closer: USA FREEDOM Act moves US toward greater compliance with human rights law," Access blog, August 21, 2014, https://www.accessnow.org/blog/2014/08/21/one-step-closer-usa-freedom-act-moves-us-toward-greater-compliance-with-hum.

6 For more on ECPA, see: http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

Obstacles to Access

Access to the internet in the United States is largely unregulated. It is provided and controlled in practice by a small group of private cable television and telephone companies that own and manage the network infrastructure. This model has been questioned by observers who have warned that insufficient competition in the ISP market could lead to some increases in the cost of access, thus adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[7] Observers have cautioned that without effective net neutrality regulations (discussed in greater detail below), the dominant companies may decide not to continue carrying 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 several other developed countries in terms of internet speed, cost, and broadband availability.[8] As of 2014, approximately 87 percent of all Americans used the internet at least occasionally at home or work,[9] but only 70 percent of adults had high-speed broadband connections at home as of September 2013.[10] While the broadband penetration rate is high by global standards, it puts the United States significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea.[11] Lack of high-speed internet access is especially prevalent in rural areas, where low population densities make it difficult for private companies to justify large investments in network infrastructure. Wired broadband service is not yet available to 7 percent of U.S. residents, mostly in rural counties.[12] A June 2013 Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) report indicated that 14 percent of rural residents in the United States lack access to fixed broadband. However, mobile broadband is increasingly available to those living in rural areas.[13]

7 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.

8 According to a study by the Organization for Economic Cooperation and Development (OECD), as of June 2013 the United States was ranked 7th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 16th, on fixed-line broadband penetration. See, OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013," accessed May 12, 2014, http://www.oecd.org/sti/broadband/1d-OECD-WiredWirelessBB-2013-06.xls.

9 Susannah Fox and Lee Rainey, "The Web at 25 in the U.S.: Summary of Findings," Pew Research Internet Project, February 27, 2014, http://www.pewinternet.org/2014/02/27/summary-of-findings-3/. According to the International Telecommunication Union (ITU), the United States had an internet penetration rate of 84 percent by the end of 2013.

10 "Broadband Technology Fact Sheet," Pew Research Internet Project, Survey completed September 2013, http://www.pewinternet.org/fact-sheets/broadband-technology-fact-sheet/.

11 OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2013," accessed May 12, 2014.

12 "Nationwide Broadband Summary," National Broadband Map, Accessed May 14. 2014, http://www.broadbandmap.gov/summarize/nationwide. See also National Broadband Map, "Broadband Statistics Report: Broadband Availability in Urban vs. Rural Areas," Report published January 2013, http://www.broadbandmap.gov/download/Broadband%20Availability%20in%20Rural%20vs%20Urban%20Areas.pdf.

13 (As defined by having the option of one or more fixed broadband providers) National Broadband Map, "Broadband Statistics Report: Broadband Availability in Urban vs. Rural Areas," Report published January 2013, http://www.broadbandmap.gov/download/Broadband%20Availability%20in%20Rural%20vs%20Urban%20Areas.pdf.

Senior citizens, Spanish-speakers, adults with less than a high school education, and those living in households earning less than US$30,000 annually are the groups least likely to use the internet.[14] In a survey conducted by the Pew Internet and American Life Project, 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 usability and price as key deterrents. Only about 17 percent of nonusers said they knew enough about technology that they could use the internet on their own.[15]

Mobile devices have become nearly ubiquitous in the United States, with 90 percent of adults owning a mobile phone and 58 percent of adults owning a smartphone.[16] Further, 68 percent of adults access the internet through mobile devices, such as smartphones or tablets.[17] Young adults, minorities, those with less than a college education, and those with lower household incomes are the most likely to say that a phone is their primary source of internet access.[18] A growing number of people use their phones to check email, visit social-networking sites such as Facebook, and engage in online commerce. This trend has prompted 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 within 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 ISPs, it has claimed jurisdiction over some internet-related issues. 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 the role of Congress to create laws that govern the internet and delegate regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

The United States is home to a thriving communications start-up community where innovators and entrepreneurs regularly offer new technological tools at no monetary cost to the public. Popular web applications such as Twitter, the video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services such as WordPress are all freely available.

While many broadband service providers operate in the United States, five of them—Comcast, AT&T, Time Warner, and Verizon, and CenturyLink—control 70 percent of the market. These companies serve a combined 60 million customers and own the majority of network cables and

14 "The Web at 25 in the U.S.: Part 1: How the Internet has Woven Itself into American Life," Pew Research Internet Project, February 27, 2014, http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/.

15 Kathryn Zickuhr, "Who's Not Online and Why," Pew Research Internet Project, September 25, 2013, http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/.

16 "The Web at 25 in the U.S.: Part 1: How the Internet has Woven Itself into American Life," Pew Research Internet Project, February 27, 2014, http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/. The International Telecommunication Union (ITU) placed the mobile phone penetration rate at 95.5 percent by the end of 2013. See: "Mobile phone subscriptions per 100 inhabitants," ITU, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

17 Susannah Fox and Lee Rainey, "The Web at 25 in the U.S.: Summary of Findings," Pew Research Internet Project, February 27, 2014, http://www.pewinternet.org/2014/02/27/summary-of-findings-3/.

18 Kathryn Zickuhr & Aaron Smith, "Digital Differences," Pew Internet and American Life Project, April 13, 2012, http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

other infrastructure.[19] Until 2005, U.S. telephone companies were required to grant other ISPs "nondiscriminatory" access to their wire networks in order to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed network owners from any 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 higher prices, fewer options for consumers, and worse service. Broadband speeds have increased, but a majority of Americans remain limited to two or fewer options when choosing a broadband provider offering at least 6 Mbps for downstream speeds and 1.5 Mbps for upstream speeds.[20]

Over the last decade, policymakers in the United States have debated the concept of net neutrality, according to which network providers must treat all content, websites, and platforms equally when managing data traffic.[21] Supporters of the principle argue that without it, ISPs would effectively be able to block certain content and applications, or give preferential treatment to some content providers for a fee, a practice that could place limitations on citizens' access to information and online services.

Although concerns about net neutrality began emerging in the early 2000s, the issue gained widespread attention in 2007 when FCC investigators found that Comcast, a cable-television company and major ISP, had begun slowing down and blocking certain types of peer-to-peer file-sharing traffic.[22] After a long court battle on the issue, a federal appeals court sided with Comcast in April 2010 and overturned the FCC's ruling against the company. The decision 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.[23]

In December 2010, the FCC issued a compromise ruling on net neutrality (known as the Open Internet Rules) that required fixed-line service providers not to block access to, or unreasonably discriminate against, lawful websites, applications, devices, or services. The rules for wireless broadband providers were much more limited, restricting only some types of blocking and saying nothing about discrimination. Under separate FCC licensing rules covering the operation of a particular range of radio communication frequencies, some wireless carriers are barred from discriminating among devices and applications, but these rules are not universally applied.[24] In 2011, advocates filed a complaint with the FCC alleging that Verizon had violated these licensing rules by demanding that certain applications (specifically, applications that enable a mobile device to create a wireless "hotspot," essentially sharing its connection with other devices) be removed from Google's

19 "Broadband Internet Penetration Deepens in the United States; Cable is King," IHS Technology, December 9, 2013, https://technology.ihs.com/468148/broadband-internet-penetration-deepens-in-us-cable-is-king.

20 "Internet Access Services: Status as of December 31, 2012," Federal Communications Commission, Published December 2013, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-324884A1.pdf (see p. 9).

21 Tim Wu, "Network Neutrality FAQ," Timwu.org, Accessed May 14, 2014, http://timwu.org/network_neutrality.html.

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

23 *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.

24 U.S. Code of Federal Regulations, Title 47, sec. 27.16, Accessed May 14, 2014, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title47/47cfrv2_02.tpl.

application store. In 2012, Verizon settled this complaint with the FCC, agreeing that the company would not restrict the availability of such applications.[25]

In a decision issued in January 2014 (*Verizon v. FCC*), the federal court of appeals in Washington DC struck down the Open Internet Rules for both fixed and mobile access providers.[26] The court ruled that the FCC does have some jurisdiction over broadband providers under a statute intended to ensure the rapid deployment of high-speed communications capability. It also found, however, that the FCC was prevented from imposing a nondiscrimination obligation on providers of broadband internet access due to its prior decisions on the regulatory classification of broadband. On May 15, 2014, the FCC opened a new consultation on the issue, but there are currently no legal protections for net neutrality in place, and it is unclear how robust and legally stable the FCC's next attempt will be.[27] The rule proposed by the FCC in May was criticized by many net neutrality proponents for not going far enough to preserve open, non-discriminatory access to content of users' choice. But, there is strong opposition in Congress and among internet service providers to the idea put forth by some net neutrality advocates that the FCC should reclassify broadband as a service that could legally be subjected to a nondiscrimination regime.[28]

Limits on Content

Access to information on the internet is generally free from government interference in the United States. There is no government-run filtering mechanism affecting content passing over the internet or mobile phone networks. Users with opposing viewpoints engage in vibrant online political discourse and face almost no legal or technical restrictions on their expressive activities online. At the same time, recent revelations about the extent of government surveillance of online communications have led some to report an increase in self-censorship.

Although the government does not restrict any political or social content, legal rules that apply to other spheres of life have been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of confidential information, 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 a sentence of up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988, 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

25 Federal Communications Commission, Consent Decree In the Matter of Cellco Partnership d/b/a Verizon Wireless, DA 12-1228, July 31, 2012, http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-12-1228A1.pdf.

26 *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014)

27 Notice of proposed rulemaking available at http://www.fcc.gov/document/fcc-launches-broad-rulemaking-protect-and-promote-open-internet.

28 Letter to FCC Chairman Tom Wheeler from members of Congress, May 14, 2014, http://www.speaker.gov/sites/speaker.house.gov/files/5-14-14-Net-Neutrality-Letter.pdf

Homeland Security, and other law enforcement agencies have asserted their authority to seize the domain name of a website allegedly hosting child abuse images after obtaining a court order.[29]

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content, such as the Child Online Protection Act of 1998 (COPA), but they have been 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 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 child pornography or visual depictions that are obscene or harmful to minors. Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, but more public libraries are seeking federal aid in order to mitigate budget shortfalls.[30] 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. However, not all libraries allow this option, arguing that the decisions about the use of filters should be left to the discretion of individual libraries.[31]

In addition to restricting access to universally illegal content such as child pornography, the government has in recent years started more aggressively pursuing alleged infringements of intellectual property rights on the internet. Since 2010, the Immigration and Customs Enforcement (ICE) 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 link to illegal copies of music and films and sites that sell counterfeit goods.[32] These seizures have been criticized as overly secretive and lacking in due process; for example, ICE seized the domain name of a legitimate hip-hop music site in November of 2010 and refused to return it for an entire year. The decision to withhold the domain was based on sealed court proceedings to which the owners of the domain were not allowed access.[33] In August 2012, three members of Congress wrote a letter to the U.S. Attorney General raising concerns about whether ICE procedures give websites meaningful due process.[34] However, ICE continues to pursue the project, which is known as "Operation in Our Sights." In December 2013, ICE announced that it partnered with 10 international law enforcement agencies to seize 706 domains allegedly selling counterfeit goods to online consumers. The U.S. component of this initiative, called "Project Cyber Monday IV," resulted in the seizure of 297 domains.[35]

29 Treating domain names as property subject to criminal forfeiture, 18 U.S.C. 2253.

30 "Public Library Funding & Technology Access Landscape 2011-2012: Public Library Funding Landscape," American Library Association, p 15, Accessed May 14, 2014, http://www.ala.org/research/sites/ala.org.research/files/content/initiatives/plftas/2011_2012/plftas12_funding landscape.pdf.

31 See, e.g., Bradburn v. North Central Regional Library District (Washington state Supreme Court) No. 82200-0 (May 6, 2010); Bradburn v. NCLR, No. CV-06-327-EFS (E.D. Wash. April 10, 2013).

32 Agatha Cole, "ICE Domain Name Seizures Threaten Due Process and First Amendment Rights" American Civil Liberties Union, June 20, 2012, https://www.aclu.org/blog/free-speech-national-security-technology-and-liberty/ice-domain-name-seizures-threaten-due

33 . Trevor Timm, "Blacklist Bills Ripe for Abuse Part II: Expansion of Government Powers," Deeplinks Blog, Electronic Frontier Foundation, December 9, 2011, https://www.eff.org/deeplinks/2011/12/blacklist-bills-ripe-abuse-part-ii-expansion-government-powers.

34 Rep. Zoe Lofgren, Rep. Jason Chaffetz, Rep. Jared Polis, Letter to Attorney General Holder and Secretary Napolitano regarding ICE domain seizures, August 30, 2012, http://www.docstoc.com/docs/128053420/Letter-to-AG-Holder-and-Sec-Napolitano-re-Domain-Name-Seizures-083012/.

35 "ICE, International Law Enforcement Agencies Seize 706 Domain Names Selling Counterfeit Merchandise," U.S. Immigration and Customs Enforcement News Releases, December 2, 2013, https://www.ice.gov/news/releases/1312/131202washingtondc.htm.

The activities of WikiLeaks, which in 2010 published several tranches of U.S. government material that was leaked by U.S. Army intelligence analyst Chelsea Manning (formerly Bradley Manning), triggered a serious debate about the use of the internet to publicize sensitive or classified government documents.[36] WikiLeaks faced the cut-off of service by non-government entities, including Amazon's data storage service[37] and EveryDNS, Wikileaks' domain name service provider.[38] While these and other companies 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.[39] Manning pleaded guilty to some charges, was convicted of others and received a lengthy sentence in August 2013. According to a *Washington Post* article published in November 2013, government officials reported that while the grand jury investigation of Wikileaks is technically ongoing, it is unlikely that the organization's leader, Julian Assange, will face charges in the United States.[40] Likewise, the Attorney General has said that the U.S. government would not prosecute Glenn Greenwald, the journalist who first published documents leaked by Edward Snowden, or "any journalist who's engaged in true journalistic activities."[41]

The legality of online gambling is another topic of debate in the United States. Online gambling is governed by a patchwork of state and federal laws. In 2011, the Justice Department delivered a legal opinion clarifying the scope of the Wire Act of 1961, which opened the door for states to legalize a number of forms of gambling, including online poker.[42] Following the opinion, Nevada, New Jersey, and Delaware legalized online gambling within their borders. Other states are considering similar legislation.[43] Some elected officials at the federal level oppose this trend. In March 2014, Senator Lindsey Graham and Congressman Jason Chaffetz introduced a bill that would reverse the Justice Department's 2011 interpretation. As of May 2014, the bill had not progressed out of committee.[44]

In November 2013, the free expression and literature advocacy group PEN America released the results of a survey showing that the NSA surveillance revelations had resulted in increased self-

36 This information included video footage of a 2007 incident in which journalists and Iraqi civilians were killed by U.S. forces, documents on the wars in Afghanistan and Iraq, diplomatic cables from the U.S. State Department, and reports on prisoners held in Guantanamo Bay military prison, all of which number in the tens and (in the case of the Iraq war) hundreds of thousands.

37 Geoffrey A. Fowler, "Amazon Says WikiLeaks Violated Terms of Service," Wall Street Journal, December 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.

38 Kevin Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities," Wired, December 3, 2010, http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.

39 Ewen MacAskill, "WikiLeaks Website Pulled by Amazon After US Political Pressure," Guardian, December 1, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

40 Sari Horowitz, "Julian Assange Unlikely to Face U.S. Charges Over Publishing Classified Documents," the *Washington Post*, November 25, 2013, http://www.washingtonpost.com/world/national-security/julian-assange-unlikely-to-face-us-charges-over-publishing-classified-documents/2013/11/25/dd27decc-55f1-11e3-8304-caf30787c0a9_story.html.

41 Sari Horowitz, "Justice is reviewing criminal cases that use surveillance gathered under FISA," Washington Post, November 15, 2013, http://www.washingtonpost.com/world/national-security/justice-reviewing-criminal-cases-that-used-evidence-gathered-under-fisa-act/2013/11/15/0aea6420-4e0d-11e3-9890-a1e0997fb0c0_story.html.

42 United States Department of Justice, Memorandum "Opinion for the Assistant Attorney General: Whether Proposals by Illinois and New York to Use the Internet and Out-of-State Transaction Processors to Sell Lottery Tickets to In-State Adults Violate the Wire Act," September 20, 2011, http://www.justice.gov/olc/opiniondocs/state-lotteries-opinion.pdf.

43 "2013 Legislation Regarding Internet Gambling or Lotteries," National Conference of State Legislatures, December 20, 2013, http://www.ncsl.org/research/financial-services-and-commerce/2013onlinegaminglegislation.aspx.

44 "Graham, Chaffetz Introduce Bipartisan Legislation to Restore Wire Act," Senator Lindsay Graham Press Release, March 26, 2014, http://www.lgraham.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=f8442c66-a918-da0c-9a4d-ddb201e26ae9.

censorship among writers. Since the revelations began in June 20013, 28 percent of respondents reported having altered or avoided social media activities, 24 percent reported deliberately avoiding certain topics in phone or email conversations, and 16 percent reported avoiding writing or speaking about a particular topic.[45] Additionally, Human Rights Watch conducted a survey of journalists and lawyers revealing the degree to which NSA surveillance has impacted their ability to communicate with sources and clients confidentially. Journalists reported that government officials are significantly less likely to speak with journalists than they were a few years ago due to concerns about anonymity and the ability of the intelligence agencies to access their communications information. Lawyers also reported facing increasing pressure to conceal or secure their communications with clients, particularly in cases with foreign governments or prosecutions that might spark an intelligence inquiry.[46]

The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen 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. Email campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and educating the public.

In 2011, technologists, digital rights advocates, companies such as Google and Mozilla, and the internet community at large came together to voice resounding opposition to two bills, the PROTECT IP Act (PIPA) and the Stop Online Piracy Act (SOPA), largely using online tools. SOPA and PIPA sought to target websites outside of the United States that host material allegedly infringing on U.S. copyrights. The bills would have permitted the Attorney General, with little judicial review, to seek orders directing ISPs to block access to domain names of sites allegedly dedicated to infringing activity, even if sites also contained lawful content. SOPA and PIPA threatened to suppress unquestionably legal speech and posed a threat to the infrastructure of the internet. Online mobilization against SOPA and PIPA was unprecedented: 10 million signatures to petitions, 4 million emails to legislators, and 115,000 sites blacking out or going dim in protest.[47] In response to these efforts and internal concerns, members of Congress withdrew the bills from consideration.

Political activity is increasingly moving online. According to a 2013 survey by the Pew Center's Internet and American Life Project, 34 percent of adults had recently contacted a government official or spoken out in a public forum using online methods. In addition, 39 percent of American adults had taken part in a political activity using a social networking site like Facebook or Twitter in the 12 months preceding the survey. Groups looking to encourage political action frequently use online tools to contact Americans; in the Pew survey, 21 percent of email users indicated that they regularly receive calls to action on social or political issues by email.[48] In addition, political candidates and

45 "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," PEN America, November 12, 2013, http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf.

46 Human Rights Watch, "How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," July 28, 2014, http://www.hrw.org/reports/2014/07/28/liberty-monitor-all.

47 "The January 18 Blackout/Strike in Numbers and Screenshots," Fight for the Future, Accessed May 14, 2014, http://sopastrike.com/numbers/.

48 Aaron Smith, "Civic Engagement in the Digital Age," Pew Research Internet Project, April 25, 2013, http://www.pewinternet.org/2013/04/25/civic-engagement-in-the-digital-age/.

elected officials at the local, state, and federal level increasingly use email, mobile apps, and online content to garner support and keep their constituents engaged.

Violations of User Rights

The United States has a robust legal framework that supports free expression rights both online and offline, and the United States does not typically prosecute individuals for online speech. The broader picture of user rights in America, however, has become increasingly complex as a series of U.S. government practices, policies, and laws touch on, and in some cases appear to violate, the rights of individuals both inside the United States and abroad. Government surveillance is a major concern, especially following revelations about NSA practices. Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has also been criticized. In addition, the privacy of NGOs, companies, and individual users is threatened by a growing number of cyberattacks initiated by both domestic and international actors.

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court held that internet speech was entitled to the highest form of protection under the constitution, and lower courts have consistently struck down attempts to regulate online content. 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. The Digital Millennium Copyright Act (DMCA) of 1998 provides a safe harbor to intermediaries that take down allegedly infringing material after notice from the copyright owner. These statutes enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.[49]

There have been concerns about cases in which law enforcement has required social media companies to turn over user information to support an investigation and forbidden the companies from disclosing any information about the subpoena to impacted users. In 2012, federal authorities issued a subpoena to the microblogging service Twitter, requesting information from the Twitter accounts of Chelsea Manning (formerly Bradley Manning), Julian Assange, and others associated with WikiLeaks. With the subpoena came a gag order compelling Twitter not to disclose this information to anyone, including the users in question. Twitter attorneys successfully challenged the gag order in court and were able to notify users before disclosing their information to government officials.[50]

In March 2014, a U.S. magistrate judge in Washington D.C. took an unusual step in a case involving secret grand jury subpoenas. The judge issued orders in two cases denying Justice Department requests for gag orders that would have prohibited Twitter and Yahoo from telling anyone, including the affected customers, that the companies had received demands for disclosure of user information. The judge specified that gag orders would not be granted until the companies had an opportunity

49 "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf.

50 Ryan Singel, "Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard," Wired, January 10, 2011, http://www.wired.co.uk/news/archive/2011-01/11/twitter-subpoena-reaction.

to respond.[51] However, a district court judge set aside the magistrate's orders.[52] The case illustrates the uneasiness among at least some federal magistrates (low level judges who handle most government applications for surveillance and access to communications data) over the exercise of the government's surveillance powers.[53]

In another concerning case regarding government access to information, the Associated Press (AP) reported in May 2013 that, as part of a national security leak investigation, the U.S. Justice Department subpoenaed and gained access to two months of phone records for several reporters following AP coverage of a failed bomb plot in Yemen.[54] Justice Department guidelines specify that, in the course of an investigation, requests for journalists' records should be "as narrowly drawn as possible," and that investigators should attempt to obtain records directly from journalists on a voluntary basis, when possible.[55] The Associated Press has since reported that the government's actions have had a chilling effect on sources, discouraging even long-standing informants from speaking with the AP.[56] In February 2014, the Attorney General signed a set of guidelines that limit the circumstances under which government may access journalists' records, but the document does not prohibit the practice entirely.[57]

Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has fueled growing criticism of that law's scope and application. Under CFAA, it is illegal to access a computer without authorization, but the law fails to define the term "without authorization," leaving the provision open to interpretation in the courts.[58] In one prominent case, programmer and internet activist Aaron Swartz secretly used Massachusetts Institute of Technology servers to download millions of files from a service providing academic articles. Prosecutors sought harsh penalties for Swartz under CFAA, which could have resulted in up to 35 years imprisonment.[59] Swartz committed suicide in early 2013. Shortly after his death, a bipartisan group of lawmakers introduced "Aaron's Law," draft legislation that would prevent the government from using CFAA to prosecute terms of service

51 Alison Frankel, "D.C. Judge Wants DOJ to Justify 'Gag Orders' on Twitter and Yahoo," Reuters, April 1, 2014, http://blogs.reuters.com/alison-frankel/2014/04/01/d-c-judge-wants-doj-to-justify-gag-orders-on-twitter-yahoo/. In a third case, the magistrate issued a detailed explanation for his conclusion that the service providers could challenge the applications for the gag orders. United States District Court for the District of Columbia, In Re Application of the United States of America for Nondisclosure Order Pursuant to Misc. Case. No. 14-480 (JMF), 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014032122836,

52 Josh Gerstein, "Leader is magistrates' 'revolt' brushed back," Politico, May 16, 2014 http://www.politico.com/blogs/under-the-radar/2014/05/leader-in-magistrates-revolt-brushed-back-188692.html?hp=r5.

53 Ann E. Marinow and Craig Timberg, "Low-level federal judges balking at law enforcement requests for electronic surveillance," Washington Post, April 24, 2014 http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html.

54 Carrie Johnson, "Justice Department Secretly Obtains AP Phone Records," National Public Radio, May 14, 2013, http://www.npr.org/2013/05/14/183810320/justice-department-secretly-obtains-ap-phone-records.

55 "Look Who's Talking: The Administration Seems to Have Trampled on Press Freedom," The Economist, May 18, 2013, http://econ.st/YN4N8n.

56 Lindy Royce-Bartlett, "Leak Probe Has Chilled Sources, AP Exec Says," The Associated Press, June 19, 2013, http://www.cnn.com/2013/06/19/politics/ap-leak-probe.

57 Charlie Savage, "Attorney General Signs New Rules to Limit Access to Journalists' Records," The New York Times, February 21, 2014, http://www.nytimes.com/2014/02/22/us/attorney-general-signs-new-rules-to-limit-access-to-journalists-records.html.

58 "Computer Fraud and Abuse Act Reform," Electronic Frontier Foundation, Accessed May 14, 2014, https://www.eff.org/issues/cfaa.

59 "Deadly Silence: Aaron Swartz and MIT," The Economist, August 3, 2013, http://www.economist.com/news/international/21582578-campaigner-academic-openness-gains-partial-posthumous-vindication-deadly-silence.

violations and stop prosecutors from bringing multiple redundant charges for a single crime.[60] As of May 2014, the bill remains stalled in the House Judiciary Committee.

In August 2011, public transit authorities in San Francisco suspended mobile phone service in several underground stations of the Bay Area Rapid Transit (BART) system in an effort to impede planned demonstrations regarding the fatal shooting of a man by BART police the month prior. Numerous digital rights advocates and First Amendment scholars called the decision a violation of BART passengers' First Amendment rights.[61] Following the incident, various civil liberties groups filed an emergency petition with the FCC requesting that the agency declare the BART shutdown a violation of the Communications Act.[62] In early 2012, the FCC issued a call for public comment on the issue, but as of mid-2014 the agency had not yet taken further action on the subject.[63] In December 2011, BART adopted a policy outlining the circumstances under which it could shut down service; the policy did not require prior judicial approval, but had it been in place, it would not have allowed for the August 2011 shutdown.[64] In September 2013, the state of California adopted legislation requiring state and local officials to obtain a court order before interfering with electronic communications systems used by the public. Certain emergency situations are exempted from this rule, which went into effect on January 2014.[65]

Although some of the most popular social media platforms in the United States require users to register and create accounts using their real names through Terms of Service or other contracts,[66] there are no legal restrictions on user anonymity on the internet. 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.[67] In April 2011, the Obama administration launched the 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

60 "Rep Zoe Lofgren Introduces Bipartisan Aaron's Law," website of Representative Zoe Lofgren, June 20, 2013, http://lofgren.house.gov/news/documentsingle.aspx?DocumentID=365647.

61 David Streitfeld, "Bay Area Officials Cut Cell Coverage to Thwart Protestors," Bits Blog, NYTimes.com, August 12, 2011, http://bits.blogs.nytimes.com/2011/08/12/bay-area-authorities-cut-cell-coverage-to-thwart-protestors/. See also, Cynthia Wong, "Welcome to San Francisco – Next Stop, Cairo?" Center for Democracy and Technology PolicyBeta Blog, August 23, 2011, http://cdt.org/blogs/cynthia-wong/238welcome-san-francisco-next-stop-cairo.

62 Mike Masnick, "FCC Asked For Declaratory Ruling That BART Shutting Off Mobile Phone Service Was Illegal," TechDirt (blog), August 31, 2011, http://www.techdirt.com/blog/wireless/articles/20110830/11591515740/fcc-asked-declaratory-ruling-that-bart-shutting-off-mobile-phone-service-was-illegal.shtml.

63 "Commission Seeks Comment on Certain Wireless Interruptions," Federal Communications Commission, March 1, 2012, http://www.fcc.gov/document/commission-seeks-comment-certain-wireless-service-interruptions.

64 Michael Cabanatuan, "BART Cellphone Shutdown Rules Adopted," SF Gate, December 2, 2011, http://www.sfgate.com/bayarea/article/BART-cell-phone-shutdown-rules-adopted-2344326.php. See also Gabe Rottman, "Shutting Down Cell Service During Protests: The Constitutional Dimension," ACLU of Northen California, May 1, 2012, https://www.aclu.org/blog/technology-and-liberty-free-speech/shutting-down-cell-service-during-protests-constitutional.

65 Bob Egelko, "New State Law Prohibits Electronic Network Shutdown," San Francisco Gate, September 26, 2013, http://www.sfgate.com/bayarea/article/New-state-law-prohibits-electronic-network-4848252.php.

66 Erica Newland, Caroline Nolan, Cynthia Wong, and Jillian York, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," Global Network Initiative, September 2011, http://cyber.law.harvard.edu/node/7080.

67 "Apple v. Does," Electronic Frontier Foundation, accessed August 1, 2012, http://www.eff.org/cases/apple-v-does.

one another's identities and systems when carrying out online transactions requiring assurance of identity.[68] The plan specifically endorses anonymous online speech.[69]

While there are no legal restrictions on anonymous communication online, there is evidence to suggest that the intelligence community in the U.S. has been working to undermine the security of anonymizing tools. Documents leaked by Edward Snowden suggest that the NSA may have been engaged in cyberattacks, including a project to develop malware targeting users of Tor (a tool that enables people to communicate anonymously online),[70] as well as efforts to undermine international technical standards for encryption.[71]

Laws that protect internet communications from government monitoring are complex. While in transit, the contents of internet communications are protected from government intrusion by constitutional rules against unreasonable searches and seizures.[72] The courts, however, have held that transactional data about communications—data showing who is communicating with whom and when—is not protected by the constitution.[73]

Under a set of complex statutes, law enforcement and intelligence agencies can monitor communications and access stored information under varying degrees of oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can monitor the content of internet communications in real time only if they have obtained an order, issued by a judge, under a standard that is actually a little higher than the one established by the constitution for searches of physical places. The order must reflect a finding that there is probable cause to believe that a crime has been, is being, or is about to be committed. The status of stored communications is more uncertain. One federal appeals court has ruled that the Constitution applies to stored communications, so that a judicial warrant is required for government access.[74] However, the Electronic Communications Privacy Act (ECPA) states that the government can obtain access to email or other documents stored in the cloud with a mere subpoena issued by a prosecutor or investigator without judicial approval.[75] As of mid-2014, advocates continue to push for reform to ECPA that would require government officials to obtain a warrant before compelling online service providers to disclose private communications, including email and documents stored using cloud

68 "About NISTIC," National Strategy for Trusted Identities in Cyberspace, Accessed May, 14, 2014, http://www.nist.gov/nstic/about-nstic.html.

69 Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" Blog of Rights (blog), American Civil Liberties Union, January 7, 2011, http://www.aclu.org/blog/technology-and-liberty/dont-put-your-trust-trusted-identities. See also, Jim Dempsey, "New Urban Myth: The Internet ID Scare," Policy Beta (blog), Center for Democracy and Technology, January 11, 2011, https://cdt.org/blog/new-urban-myth-the-internet-id-scare/.

70 Glenn Greenwald, "NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users," the *Guardian*, October 4, 2013, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

71 Glenn Greenwald, Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security, the *Guardian,* September 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

72 Paul Ohm, "Court Rules Email Protected by Fourth Amendment," Freedom to Tinker, December 14, 2010, http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment.

73 "ECPA: About the Issue," Digital Due Process, accessed April 23, 2013, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

74 United States v. Warshak, 09-3176, United States Court of Appeals for the Sixth Circuit.

75 Ibid.

services.[76] The Senate Judiciary Committee passed a reform bill in 2013, and in the House a bill to update ECPA has been cosponsored by over 260 representatives from both parties. A report produced by the White House in May 2014 offered support for ECPA reform.[77] Despite these promising signs, the Securities and Exchange Commission (SEC), a civil regulatory agency, has complicated the issue by attempting to amend the bill to secure the authority to obtain stored email and other documents directly from service providers without a warrant.[78]

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which expanded some of the government's surveillance and investigative powers in cases involving terrorism as well as in ordinary criminal investigations. Three expiring provisions of the PATRIOT Act—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 with court orders issued on a broad standard (Section 215)—were renewed for an additional four years in May 2011.[79]

However, starting in June 2013, it became clear that the issues debated in connection with the PATRIOT Act were only the tip of the iceberg in relation to U.S. government surveillance. That month, the *Guardian*, the *Washington Post,* and other news outlets revealed a series of secret documents[80] leaked by former National Security Agency (NSA) contractor Edward Snowden that provided new information (and raised many new questions) about surveillance activities conducted by the U.S. government.

Leaked documents indicated that the Foreign Intelligence Surveillance Court (FISA Court) had interpreted Section 215 of the PATRIOT Act to permit the FBI to obtain orders that compel the largest telephone carriers in the United States (Verizon, AT&T, Sprint, and presumably others) to provide the NSA with records of all phone calls made to, from, and within the country on an ongoing basis. These billions of call records include numbers dialed, length of call, and other "metadata."[81] Data are gathered in bulk, without any particularized suspicion about an individual, phone number, or device. Without approval from the FISA Court or any other judicial officer, NSA analysts conduct queries on this data, generating contact chains that show the web of connections emanating from a single phone number suspected of being associated with terrorism.[82]

---

76 Greg Nojeim, "Senate 'Dream Team' Introduced ECPA Reform Bill," Center for Democracy and Technology PolicyBeta Blog, March 19, 2013, https://www.cdt.org/blogs/greg-nojeim/1903senate-dream-team-introduces-ecpa-reform-bill. See also "ECPA: About the Issue," Digital Due Process, accessed April 23, 2013, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

77 "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p. 60 http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. See Mark Stanley, "White House Report Supports ECPA Reform," Center for Democracy and Technology PolicyBeta Blog, May 1, 2014, https://cdt.org/blog/white-house-report-supports-ecpa-reform/.

78 Greg Nojeim, "SEC Tries to Weaken Important ECPA Reform," Center for Democracy and Technology PolicyBeta Blog, July 29, 2013, https://cdt.org/blog/sec-tries-to-weaken-important-ecpa-reform/. See also Kate Tummarello, "SEC Defends Email Privacy Practices," The Hill, April 2, 2014, http://thehill.com/policy/technology/202429-sec-defends-email-privacy-practices.

79 "Patriot Act Excesses," New York Times, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.

80 E.g. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

81 For more information on privacy and metadata, see Aubra Anthony, "When Metadata Becomes Megadata: What Government Can Learn," Center for Democracy and Technology PolicyBeta Blog, June 17, 2013, https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata.

82 "Comparing Two Secret Surveillance Programs," The New York Times, June 7, 2013, http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html.

Leaks also revealed new details about programs authorized by Section 702 of the Foreign Intelligence Surveillance Act. Section 702 allows the NSA to conduct surveillance of people who are not U.S. citizens and who are reasonably believed to be located outside the United States in order to collect "foreign intelligence information."[83] Under a program called "PRISM," the NSA has been compelling at least nine large U.S. companies, including Google, Facebook, Microsoft and Apple, to disclose content and metadata relating to emails, web chats, videos, images, and documents.[84] Also under Section 702, the NSA taps into the internet backbone for "collection of communications on fiber cables and infrastructure as data flows past."[85] Although these programs are targeted at persons abroad, the NSA is able to retain and use information "incidentally" collected about U.S. persons.

Meanwhile, Executive Order 12333[86] offers the legal basis for additional surveillance programs outside the scope of FISA. Executive Order 12333 specifically addresses surveillance conducted abroad that targets non-U.S. persons (those who are not U.S. citizens or permanent resident aliens) located outside the United States. There is limited public information about how Executive Order 12333 has been interpreted by government officials, but the surveillance procedures issued under the Executive Order are designed to provide protections to U.S. citizens and residents, not to others who may be put under surveillance.[87] The Executive Order authorizes surveillance of people outside the U.S. on a very broad scale: the "foreign intelligence information" that can be sought with surveillance includes information about "the capabilities, intentions, or activities" of foreign organizations or persons.

Surveillance activities likely conducted under Executive Order 12333 authority include: bulk collection of location data from cell phones;[88] bulk collection of text messages;[89] bulk collection of contact lists from personal email and instant message accounts;[90] collection of mass amounts of data flowing between data centers of major technology companies such as Google and Yahoo;[91] and collection of user data available from mobile phone applications, including geographic data, address

83 4 Sec. 702 was adopted in 2008 as part of the FISA Amendments Act, Pub. L. 110-261, https://www.govtrack.us/congress/bills/110/hr6304

84 "NSA Slides Explain the PRISM Data Collection Program," Washington Post, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

85 James Bell, "NSA's Prism Surveillance Program: How it Works and What it Can Do," *The Guardian*, June 8, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

86 The text of Executive Order 12333 is available at: https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

87 See, for example, http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf and http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

88 Barton Gellman and Ashkan Soltani, "NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show," the *Washington Post*, December 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

89 James Ball, "NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep," *The Guardian*, January 16, 2014, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

90 Barton Gellman and Ashkan Soltani, "NSA Collects Millions of E-mail Address Books Globally," the *Washington Post*, October 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

91 Barton Gellman and Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," the *Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

books, "buddy lists," and telephone logs.[92] Critics assert that the secret NSA programs violate the Fourth Amendment, which protects people inside the United States (citizens and non-citizens alike) from unreasonable search and seizure, as well as human rights enshrined in international agreements. The Snowden leaks have prompted significant mobilization by civil society[93] and companies.[94]

Over the last year there have been some positive developments. In January 2014, the president announced that he intended to end the bulk collection of telephony metadata.[95] As of May 2014, however, the program was still operating, as Congress debated legislation to end it.[96] In January, the president also issued a policy directive that put in place important new restrictions on the use of information collected in bulk for foreign intelligence purposes.[97] The restrictions apply to communications data regarding all persons, "whatever their nationality and regardless of where they might reside." However, the restrictions do not apply to data collected under Section 702 because it is not considered a bulk collection program.[98]

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.[99] The FBI has repeatedly requested that the law be expanded to impose design requirements on online communications tools such as Gmail, Skype, and Facebook.[100] In May 2013, a group of 20 technical experts published a paper explaining why such a proposal (known as "CALEA II") would create significant internet security risks.[101] Following the leaks about NSA surveillance, focus in Washington shifted away from CALEA II, but it is possible that similar proposals will emerge in the future.

92 James Glanz, Jeff Larson, and Andrew Lehren, "Spy Agencies Tap Data Streaming from Phone Apps," The New York Times, January 27, 2014, http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?r=0.

93 See for example https://optin.stopwatching.us/ and https://en.necessaryandproportionate.org/take-action/digiges. See also https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf.

94 See for example https://www.reformgovernmentsurveillance.com/.

95 "Remarks by the President on Review o Signals Intelligence," January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence; FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program (March 27, 2014) http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m

96 "House Judiciary Passes USA FREEDOM Act," Center for Democracy and Technology Press Release, May 7, 2014, https://cdt.org/press/house-judiciary-passes-usa-freedom-act/.

97 Presidential Policy Directive – Signals Intelligence Activities (PPD-28), January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

98 During the PCLOB's March 19 public hearing on Section 702, government officials maintained that surveillance pursuant to Section 702 is not bulk collection and that this rule does not apply to such surveillance. See generally, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014, http://www.pclob.gov/Library/20140319-Transcript.pdf.

99 The FCC does not classify Skype as an "interconnected VoIP" service.

100 Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet." The New York Times, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all. See also Declan McCullagh, "FBI: We Need Wiretap-Ready Websites – Now," CNET, May 4, 2012, http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now.

101 Ben Adida et al, "CALEA II: Risks of Wiretap Modifications to Endpoints," May 17, 2013, available at https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

Law enforcement agencies have also used open, public websites and social media platforms to monitor different groups for suspected criminal activity. One notable example that generated controversy was an initiative by the New York Police Department (NYPD), uncovered in February 2012, to monitor Muslim student groups at various universities in the northeastern United States. The Associated Press reported that, from 2006 onward, the NYPD Cyber Intelligence unit had monitored blogs, websites, and online forums of Muslim student groups and produced a series of secret "Muslim Student Association" reports describing group activities, religious instruction, and the frequency of prayer by the groups.[102] Muslim students from across the nation expressed concern about this type of surveillance and told Freedom House that they often self-censor when conducting online activities. In April 2014, the NYPD closed down one unit that monitored locations associated with the Muslim community, including mosques and businesses. Civil liberties advocates welcomed this step but warned that other NYPD units may still be using discriminatory practices.[103]

Like most other countries, the United States faces the growing challenge of addressing cyberattacks conducted by both state and non-state actors. In response to concern about cybersecurity threats, President Obama produced an executive order in 2013 recognizing the need for improved cybersecurity measures and calling for a new "Cybersecurity Framework" to address security threats.[104] The executive order directed agencies to "ensure" that privacy and civil liberties protections are incorporated into their cybersecurity activities, and it specified that such protections shall be based on the Fair Information Practice Principles, an internationally recognized framework for privacy protection. At the same time, the U.S. military admitted that it is developing the ability to carry out offensive cyberattacks.[105] The documents leaked by Edward Snowden included a Presidential Policy Directive describing U.S. "Offensive Cyber Effects Operations (OCEO)."[106]

China is one focal point of the cybersecurity discussion, especially following a report by computer security firm Mandiant stating that many attacks against U.S. organizations, companies, and government agencies appear to have originated in an office of the Chinese People's Liberation Army in Beijing.[107] Following tense exchanges on the issue in 2013, the United States attempted to open a dialogue with China about cybersecurity. In early 2014, U.S. officials held a briefing for Chinese military leadership on the Pentagon's cybersecurity tactics and policy, including both offensive and defensive programs. The purpose of the briefing was to build trust and encourage reciprocity from the Chinese government.[108]

---

102 Chris Hawley, "NYPD monitored Muslim students all over Northeast," The Associated Press, February 18, 2012, http://www.ap.org/Content/AP-In-The-News/2012/NYPD-monitored-Muslim-students-all-over-Northeast

103 Noa Yachot, "NYPD Shutters Muslim Mapping Unit – But What About Other Tactics?" American Civil Liberties Union, April 15, 2014, https://www.aclu.org/blog/national-security-religion-belief/nypd-shutters-muslim-spying-unit-what-about-its-tactics.

104 "Executive Order – Improving Critical Infrastructure Cybersecurity," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

105 Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," The New York Times, March 12, 2013, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all.

106 Glenn Greenwald and Ewen MacAskill, "Obama Orders U.S. to Draw Up Overseas Target List for Cyberattacks," the *Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

107 David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit is Seen as Tied to Hacking Against the U.S." The New York Times, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&gwh=24BE5E3C317441D6CAB213658308303F&_r=0.

108 David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," The New York Times, April 7, 2014, http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html.

In March 2014, the United States government reported that it had notified 3,000 companies over the last year that their technology systems were under attack. This number represents only a small fraction of all cybersecurity threats to U.S. businesses and their customers but points to the seriousness of the problem.[109] One of the most significant attacks in 2013 targeted the financial services industry, using denial-of-service attacks to reduce availability of networks and services.[110] While some attacks target whole networks or industries, others focus on individual internet users. For example, the Ethiopian government allegedly installed surveillance spyware on the computer of a U.S. citizen living in Maryland in order to monitor his activity over a period of months. With the assistance of the Electronic Frontier Foundation, the man is suing the Ethiopian government in a United States court for illegal wiretapping.[111] Similar surveillance software appears to be used by governments around the globe.[112]

109 Ellen Nakashima, "U.S. Notified 3,000 Companies in 2013 About Cyberattacks," *The Washington Post*, March 24, 2014, http://www.washingtonpost.com/world/national-security/us-notified-3000-companies-in-2013-about-cyberattacks/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html.

110 James R. Clapper, "Worldwide Threat Assessment of the U.S. Intelligence," Senate Select Committee on Intelligence, January 29, 2014, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

111 "Kidane v. Ethiopia," Electronic Frontier Foundation, Accessed May 14, 2014, https://www.eff.org/cases/kidane-v-ethiopia.

112 See for example: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.