Freedom House

United States

	2014	2015
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	3
Limits on Content (0-35)	2	2
Violations of User Rights (0-40)	13	14
TOTAL* (0-100)	**19**	**19**

* 0=most free, 100=least free

Population:	**318 million**
Internet Penetration 2014:	**87 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2015 Status:	**Free**

Key Developments: June 2014 – May 2015

- In February 2015, the Federal Communications Commission approved new rules that allow it to regulate the internet as a public utility, including provisions to protect net neutrality (see **Media, Diversity, and Content Manipulation**).
- Members of the government have increasingly called for restrictions on encrypted communications, citing national security and intelligence concerns, while some legislators have taken steps to rebuff these efforts by introducing a bill that would prevent the government from requiring private companies to install encryption "backdoors" (see **Surveillance, Privacy, and Anonymity**).
- Online journalists and protestors filming police interactions in Ferguson, Missouri, were subject to arrest, intimidation, and harassment by police (see **Prosecutions and Detentions for Online Activities** and **Intimidation and Violence**).

Introduction

The United States took a significant step toward protecting the free and open internet in February 2015, when the Federal Communications Commission (FCC) adopted strong, bright-line network neutrality rules, which limit the extent to which internet service providers (ISPs) can pick and choose the content that reaches their subscribers. Net neutrality has dominated internet policy debates in the United States for the better part of a decade, but truly emerged as a subject of widespread public discussion in 2014, after a federal court vacated most of the FCC's 2010 Open Internet Order in response to a lawsuit led by Verizon, one of the nation's largest telecommunications companies. Following the court's January 2014 ruling, thirteen months of vigorous public debate — including the submission of over four million comments[1] through the FCC's online public notice and comment process — culminated in the FCC's decision to legally classify broadband as a telecommunications service, which in turn enabled it to approve new rules that prohibit blocking and unreasonable discrimination of content on both fixed and wireless networks.[2] Those rules are currently in effect, although several broadband companies and their trade associations have sued the FCC in federal court once again to overturn the rules.

Some progress has also been made on important issues like surveillance reform. After months of public advocacy from privacy watchdogs, technology companies, and legal experts, three key sections of the PATRIOT Act expired on June 1, 2015, which prompted Congress to finally pass the USA FREEDOM Act the following day.

At the same time, however, 2015 witnessed the development of some concerning new threats to secure and anonymous speech online. Following major product announcements by Apple and Google in September 2014, a debate emerged between law enforcement officials, technology experts, and privacy advocates about whether companies should be allowed to market products with strong encryption that do not preserve the government's ability to access decrypted versions of those encrypted communications. High-ranking officials including the FBI Director, the Attorney General, and the Director of the NSA have called on technology companies to find a technical solution to the problem, threatening to seek congressional action if necessary. There have been no actual legislative changes regarding the use of encryption at this time, but the debate has raised serious concerns about the security, free speech, and economic impact if such policies were to be put into place.

Additionally, more reports of police detaining, harassing, and threatening individuals—including professional journalists—for documenting police actions on smartphones or with cameras has called into question the degree to which this right is fully protected. Journalists for online publications were harassed and temporarily detained during demonstrations in Ferguson, Missouri, where people gathered to protest police violence against the black community in the United States.

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

1 Gigi B. Sohn and Dr. David A. Bray, "Setting the Record Straight on Open Internet Comments," *Official FCC Blog*, Federal Communications Commission, December 23, 2014, http://fcc.us/1A6hhKx.

2 Federal Communications Commission, "Report and Order on Remand, Declaratory Ruling, and Order: In the Matter of Protecting and Promoting the Open Internet," GN Docket No. 14-28, February 26, 2015, http://bit.ly/1NOC8bv.

network infrastructure. This model has been questioned by observers who warn 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.[3] *In 2015, however, several important victories for consumers — including the historic net neutrality decision and the collapse of a proposed merger between internet service giants Comcast and Time Warner Cable — suggest that the climate may be improving.*

Availability and Ease of Access

Although the United States is one of the most connected countries in the world, the speed, affordability, and availability of its broadband networks has fallen behind several other developed countries. According to the International Telecommunication Union, internet penetration in the United States reached 87 percent by the end of 2014.[4] Broadband adoption rates are high, with approximately 80 percent of Americans subscribing to either a home-based or smartphone-based internet service as of 2013.[5] While the broadband penetration rate is high by global standards, it still puts the United States significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea.[6] Moreover, access, cost, and usability remain barriers for many Americans — particularly senior citizens, people who live in rural areas, and low-income households. However, recent data from the Pew Research Center shows that internet access rates for those 65 years of age and older has steadily increased over the past decade, with more 58 percent of individuals in this age bracket using the internet as of 2015.[7]

In January 2015, the Federal Communications Commission (FCC) updated its definition of the term "broadband" to a new benchmark of 25 Megabits per second (Mbps) download and 3 Mbps upload, citing advances in technology, market offerings, and consumer demand. This change is an increase from the previous 4 Mbps download and 1 Mbps upload standard adopted in 2010. Under the new definition, the FCC found that 17 percent of the population lacks access to broadband service. Lack of access is especially prevalent in rural areas, where low population densities make it less appealing for private companies to make large investments in network infrastructure. As a result, less than half of residents in rural areas have access to 25 Mbps broadband service[8] and at least two million Americans still subscribe to dial-up internet in 2015.[9]

Despite a lack of penetration in rural areas, uptake rates for internet-enabled mobile devices have increased dramatically throughout the United States in recent years. In 2014, 90 percent of adults

3 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).

4 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2014," July 2014, http://bit.ly/1FDwW9w.

5 Kathryn Zickuhr and Aaron Smith, *Home Broadband 2013*, Pew Research, August 26, 2013, http://pewrsr.ch/N8OznH.

6 OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2014," December 2014, http://bit.ly/1cP4RGV; "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2014."

7 Andrew Perrin and Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center: Internet, Science & Tech, June 26, 2015, http://pewrsr.ch/1TRMM48.

8 Federal Communications Commission, "FCC Finds Broadband Deployment Not Keeping Pace," press release, January 29, 2015,http://bit.ly/1hIlXGf; Federal Communications Commission, *2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment*, January 29, 2015, http://bit.ly/1Lbtgbk.

9 Alison Griswold, "2 Million Americans Still Use AOL's Dial-Up Internet," *Future Tense* (blog), *Slate*, May 13, 2015, http://slate.me/1A0VuXj.

reported that they own a mobile phone, and 64 percent of adults own a smartphone.[10] 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. Recent reports by Pew Research indicate that young adults, minorities, and those with lower household incomes are more likely to be "smartphone-dependent," with limited options for internet access other than their phones.[11]

Restrictions on Connectivity

Internet users in the United States face few government-imposed restrictions on their ability to access content online. The backbone infrastructure is owned and maintained by private corporations, including AT&T and Verizon. In contrast to countries with only a few connections to the backbone internet infrastructure, the United States has numerous connection points, which would make it nearly impossible to disconnect the entire country from the internet.

At the same time, law enforcement agencies in the United States are known to have and occasionally wield the power to inhibit wireless internet connectivity to respond to emergency situations. The federal government has a non-public protocol for shutting down wireless internet connectivity in response to particular events, some details of which recently came to light following a lawsuit brought under the Freedom of Information Act.[12] The protocol, known as Standard Operating Procedure (SOP) 303, was secretly established in 2006 on the heels of a 2005 cellular-activated subway bombing in London. SOP 303 codifies the "shutdown and restoration process for use by commercial and private wireless networks during national crisis." However, what constitutes a "national crisis," and what safeguards exist against abuse remain largely unknown, as the full SOP 303 documentation has never been released to the public.[13] State and local law enforcement also have tools to jam wireless internet. For example, in 2011, San Francisco public-transit provider Bay Area Rapid Transit (BART) interrupted wireless service on its platforms to disrupt protests sparked by the police shooting of a homeless man named Charles Hill.[14] In December 2014, the FCC issued an Enforcement Advisory clarifying that it is illegal to jam cell phone networks without a federal authorization, even for state and local law enforcement agencies.[15]

ICT Market

There are few obstacles that prevent the existence of diverse business entities providing access to digital technologies in the United States, which is home to a thriving startup community of innovators and entrepreneurs that has produced many low-cost, globally successful online platforms and tools.

10 Aaron Smith, *Smartphone Use in 2015*, Pew Research, http://pewrsr.ch/19JDwMd.

11 Aaron Smith, *Smartphone Use in 2015*, Pew Research, http://pewrsr.ch/19JDwMd.

12 The Electronic Privacy Information Center (EPIC) filed suit against the Department of Homeland Security (DHS) in 2013 for information about the protocol. After winning an appeal in the DC Circuit, the DHS retained exemption from disclosing SOP 303, and in July of 2015 released a redacted version of the protocol. Electronic Privacy Information Center, *EPIC v. DHS – SOP 303,* http://bit.ly/1GscPWS; Electronic Privacy Information Center, *SOP 303 Updated Release*, http://bit.ly/1WI9hZV.

13 Electronic Privacy Information Center, *EPIC v. DHS – SOP 303*.

14 Melissa Bell, "BART San Francisco Cut Cell Services to Avert Protest," *The Washington Post*, August 12, 2011, http://wapo.st/1GscX8T

15 Federal Communications Commission, *WARNING: Jammer Use Is Prohibited*, December 8, 2014, http://fcc.us/1L1RV2O.

While there are many broadband service providers operating in the United States, the industry has trended toward consolidation. Five dominant providers — Comcast, AT&T, Time Warner Cable, Verizon, and CenturyLink — own the majority of network cables and other infrastructure, serving a combined 65 million customers and controlling 70 percent of the market for 4 Mbps service.[16] For customers subscribing to service that meets the new 25 Mbps benchmark for broadband, the market is even less competitive, with a single provider — Comcast — controlling over 50 percent of the market.[17]

In 2005, the FCC embraced an aggressive deregulation agenda that freed network owners from a longstanding obligation to lease their lines to competing providers. Deregulation proponents claimed that this step would give large cable and telephone companies incentive to expand and upgrade their networks, while opponents worried that the move would lead to higher prices, fewer options for consumers, and worse service. Although average broadband speeds have increased over the past decade, the majority of American households have access to only one broadband provider that offers download speeds of at least 25 Mbps, and nearly 20 percent of Americans have no option at all for internet access at this speed.[18]

Americans increasingly access the internet via mobile technologies, as wireless carriers deploy advanced Long-Term Evolution (LTE) networks. Following a decade of consolidation, the U.S. wireless market is dominated by four national carriers — AT&T, Verizon, Sprint, and T-Mobile — that reach 99 percent of Americans.[19] The U.S. government has looked unfavorably on further consolidation, notably when regulators blocked AT&T's proposed merger with T-Mobile in 2011 and when regulators signaled that they would block a rumored Sprint/T-Mobile merger in 2014.[20] Moreover, the government promoted the growth of mobile broadband through a series of recent spectrum auctions, including a successful auction in late 2014 and a planned auction in early 2016.

Within the past year, the U.S. government has taken steps to encourage broadband competition. In April 2015, federal regulators at the FCC and the U.S. Department of Justice indicated they would block a proposed merger between Comcast and Time Warner Cable, citing concerns that the combined company would have too much influence over the broadband market.[21] The companies subsequently abandoned the transaction. In January 2015, President Barack Obama announced an initiative to encourage the development of community-based broadband services and asked the FCC to remove barriers to local investment.[22] One month later, the FCC "preempted," or overturned, state laws in Tennessee and North Carolina that restrict local broadband services, arguing that such laws

16 Leichtman Research Group, "3 Million Added Broadband From Top Providers in 2014," press release, March 5, 2015, http://bit.ly/1WIa1hL.

17 Jon Brodkin, "Comcast now has more than half of all US broadband customers" *Ars Technica*, January 30, 2015, http://bit.ly/1FPGOgI.

18 Prepared Remarks of Federal Communications Commission Chairman (FCC) Tom Wheeler "The Facts and Future of Broadband Competition". September 4, 2014 https://apps.fcc.gov/edocs_public/attachmatch/DOC-329161A1.pdf .

19 Federal Communications Commission, *Mobile Wireless Competition Report*, December 18, 2014, http://bit.ly/1EJS5tz.

20 Michael J. De La Merced, "Sprint and Softbank End Their Pursuit of a T-Mobile Merger," *DealB%k* (blog), *New York Times*, August 5, 2014, http://nyti.ms/1KW0LBh.

21 Federal Communications Commission, "Statement from FCC Chairman Tom Wheeler on the Comcast-Time Warner Cable Merger," news release, April 24, 2015, http://bit.ly/1OfzSug ; U.S. Department of Justice, "Comcast Corporation Abandons Proposed Acquisition of Time Warner Cable After Justice Department and Federal Communications Commission Informed Parties of Concerns," press release, April 24, 2015, http://1.usa.gov/1Qrf57U.

22 The White House, Office of the Press Secretary, "FACT SHEET: Broadband That Works: Promoting Competition & Local Choice In Next-Generation Connectivity," press release, January 13, 2015, http://1.usa.gov/1GUJIQ9.

create barriers to broadband deployment.[23] However, that action is currently being challenged in federal court and similar laws remain valid in many other states.

Regulatory Bodies

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency, is charged with regulating radio and television broadcasting, interstate communications, and international telecommunications that originate or terminate in the United States. The FCC has jurisdiction over a number of internet-related issues, especially in light of the February 2015 decision to reclassify broadband as a telecommunications service under the Communications Act. Other government agencies, such as the Commerce Department's 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.

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. Additionally, the FCC's decision in February 2015 to approve net neutrality rules will ensure that ISPs cannot discriminate against traffic based on content. At the same time, recent revelations about the extent of government surveillance of online communications and aggressive investigations into journalists in whistleblower cases have led some to report an increase in self-censorship over the past few years.

Blocking and Filtering

In general, the U.S. government does not block or filter online content. Some states require publicly funded schools and public libraries to install filtering software on their computers to block obscene, illegal, or harmful content.[24] However, the rise of the Islamic State has sparked intense debate about the appropriate role of social media companies in combating the use of mainstream social media as a tool used by terrorist organizations for recruitment and communication. Some government officials say that social media companies are being exploited by terror organizations, and that the companies have an active responsibility to block or remove terror-related content.[25] Various companies maintain their own internal trust and safety policies with regard to hate speech and extremist groups, and in July 2015, the Senate Intelligence Committee approved legislation in a closed hearing that would require "electronic communication service providers" to report suspected terrorist content to

23 Federal Communications Commission, "FCC Grants Petitions to Preempt State Laws Restricting Community Broadband in North Carolina, Tennessee," news release, February 26, 2015, http://bit.ly/1Z3DrZO.

24 National Conference of State Legislators, "Laws Relating to Filtering, Blocking, and Usage Policies in Schools and Libraries," June 12, 2015, http://bit.ly/1zvIfGT.

25 Scott Higham and Ellen Nakashima, "Why the Islamic State leaves tech companies torn between free speech and security," *Washington Post,* July 16, 2015, http://wapo.st/1O9SVUQ.

federal authorities.[26]

Content Removal

Illegal online content—including child pornography and content that infringes on copyright—hosted within the United States can be removed through a court order or similar legal process. However, aside from these examples of illegal content, government pressure on ISPs or content hosts to remove content is not a widespread issue within the United States.

One of the most important protections for online free expression in the United States is Section 230 of the Communications Decency Act (CDA 230), which generally shields online sites and services from legal liability for the activities of their users, thus allowing sites and services with rich user-generated content to flourish.[27] However, although the government does not censor any particular political or social viewpoints, legal rules do restrict certain types of content on the internet, and there have even been some attempts to step back the broad protections of CDA 230. For example, concerns over intellectual property violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of commercial trade secrets, 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 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.[28]

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content online, such as the Child Online Protection Act of 1998 (COPA), but these laws have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedom 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.[29] 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 individu-

26 Ellen Nakashima, "Lawmakers want Internet sites to flag 'terrorist activity' to law enforcement," *Washington Post*, July 4, 2015, http://wapo.st/1H9hEq9.

27 47 U.S.C. §230 (1998), http://bit.ly/1hlnlbP; *see* Electronic Frontier Foundation, "Section 230 of the Communications Decency Act," http://bit.ly/1EYGbk1.

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

29 American Library Association, "Public Library Funding Landscape," 2011-2012, accessed June 4, 2015, 15, http://bit.ly/1KW2uql.

al libraries.[30]

Congress is also considering passing a law known as the SAVE Act, which would help protect against sex trafficking of children by making it a serious criminal offense to knowingly advertise a sex trafficking victim, or to benefit from such advertising.[31] A number of civil society groups have pushed back against the proposed law, arguing that the associated harsh penalties would chip away at CDA 230 protections, chill a robust advertising ecosystem that is generally content neutral, and encourage online websites and services to self-censor.[32] As of May 2015, the SAVE Act has passed in the House of Representatives and is under consideration in the U.S. Senate.

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, as well as sites that sell counterfeit goods.[33] These seizures have been criticized as overly secretive and lacking in due process, Nevertheless, ICE continues to pursue the project, which is known as "Operation In Our Sights."[34] 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 resulted in the seizure of 297 domains. In December 2014, the partnership announced the seizure of an additional 292 domains, bringing the total number of seizures so far to 1,829.[35]

Not only is the ICE now involved in interfering with online content that implicates intellectual property rights, but last year the International Trade Commission (ITC), a trade agency that can block the importation of articles that infringe intellectual property, joined the fray. The ITC normally deals with the importation of physical articles, but in an unprecedented move in 2014, the ITC declared that it had the authority to block the cross-border transmission of data violating a U.S. patent.[36] In a letter to the ITC, a number of civil society groups and academic scholars urged the ITC to reconsider its stance that it can block pure data transmissions, cautioning that the "decision has enormous ramifications, opening the door to internet content blocking efforts rejected by Congress and the public."[37] The ITC paused on action pending a Federal Circuit ruling on the case.[38]

For copyright infringement claims, the removal of online content is dictated by the safe harbor provisions created in Section 512 of the Digital Millennium Copyright Act (DMCA).[39] Operating through a "notice-and-takedown" mechanism, ISPs are shielded from liability if they remove infringing content upon receipt of a DMCA notice. However, because ISPs have the incentive to err on the side of

30 *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).

31 H.R. 285, https://www.congress.gov/114/bills/hr285/BILLS-114hr285rfs.pdf.

32 Center for Democracy & Technology, "Coalition Statement in Opposition to Federal Criminal Publishing Liability," January 29, 2015, http://bit.ly/1OSYquU.

33 Agatha Cole, "ICE Domain Name Seizures Threaten Due Process and First Amendment Rights, " American Civil Liberties Union, June 20, 2012, http://bit.ly/1j9cXpl.

34 U.S. Immigration and Customs Enforcement "Operation In Our Sites," May 22, 2014, http://1.usa.gov/1WIeTn7.

35 Europol, "292 Internet Domain Names Seized for Selling Counterfeit Products," December 1, 2014, http://bit.ly/1Q1b6x5.

36 United States International Trade Commission, "Certain Digitals Models, Digital Data, and Treatment Plans for Use in Making Incremental Dental Positiong Adjustment Applicances, The Appliances Made Therefrom, and Methods of Making the Same," commission opinion, April 10, 2014, http://bit.ly/1Pf0nky.

37 "Letter to the International Trade Commission," Public Knowledge, April 10, 2015, http://bit.ly/1Z3Ih9u.

38 Public Knowledge, "Brief of PK and EFF in ClearCorrect v. ITC," October 16, 2014, http://bit.ly/1VBdrQP.

39 17 U.S.C.§ 512, https://www.law.cornell.edu/uscode/text/17/512.

caution and remove any hosted content subject to a DMCA notice, there have been occasions where overly broad or fraudulent DMCA claims have resulted in the removal of content that would otherwise be excused under free expression, fair-use, or educational provisions.[40]

In recent years, a number of internet companies have taken to publicly reporting requests to remove content. Many of these reports focus on trademark-related requests or requests alleging copyright infringement under the DMCA. There is also some concern regarding the intellectual property sections of the Trans-Pacific Partnership, and whether the proposed trade agreement would extend portions of U.S. copyright terms internationally.[41]

In 2012, Google started reporting information about the copyright removal notices it receives, including how often notices are received, the names of the copyright owners or their agents who submit the requests, and the websites identified.[42] The company also reports on how often infringing links are removed from search results. A number of other major internet companies, including Twitter, Automattic (publisher of Wordpress.com), and the Wikimedia Foundation, similarly report on intellectual property takedowns. Companies have also expanded their practices to include their compliance rates and, in some cases, information about the links or content the company did not remove because it was deemed non-infringing. Transparency around unactionable DMCA claims may become increasingly popular in light of the number of abuses of the copyright takedown system.

While reporting on copyright removal requests is growing, so too is the practice of reporting on government requests to remove content. Major internet companies, including Twitter, Facebook, Yahoo, and Pinterest, publicly share information about these requests, which come from around the world. According to Twitter, "[g]overnments generally make removal requests for content that may be illegal in their respective jurisdictions," such as hate speech, defamatory statements, or child pornography.[43] According to the latest data publicly released by Twitter, between July and December of 2014, the social media company received 6 court orders and 26 U.S. government requests to remove or withhold content, although the company also reported zero percent compliance for the 32 requests.[44] In 2014, Yahoo received 5 U.S. government removal requests for a total of 11 items and complied with 4 of the 5 requests. The company reports that it did not comply with "a court order from a U.S. government agency to remove content" because the company "did not host any of the domains or content."[45]

Media, Diversity, and Content Manipulation

The online environment in the United States is vibrant, diverse, and generally free of economic or political constraints. Anyone can start a blog, forum, or social media site to discuss opinions and share news and information. Due to the FCC's decision to protect net neutrality regulations, ISPs cannot throttle, block or otherwise discriminate against internet traffic based on its content. Self-censorship, however, continues to exist to some degree due to the extensive government surveillance revealed over the past two years.

40 Electronic Frontier Foundation, "Lenz v. Universal," https://www.eff.org/cases/lenz-v-universal.

41 TorrentFreak, TPP: U.S. May Not Force DMCA on Other Countries https://torrentfreak.com/tpp-u-s-may-accept-partners-own-isp-liability-frameworks-150707/.

42 "Transparency for copyright removals in search," *Google Official Blog*, March 24, 2012, http://bit.ly/1L1WABP.

43 Twitter , "Removal Requests," *Transparency Report,* July-December, 2014, http://bit.ly/1wZlsZK.

44 Ibid.

45 Yahoo!, "Government Removal Requests," *Transparency Report*, http://bit.ly/1GZ3HMU.

The concept of network neutrality — a foundational principle of the internet that prohibits network operators from giving preferential treatment to favored content or from blocking disfavored content — has dominated internet policy debates in the United States for the better part of a decade. The issue emerged in the early 2000s and gained widespread attention in 2008 when the FCC penalized Comcast, a major American broadband provider, for throttling a file-sharing application called BitTorrent.[46] A federal court later overturned the FCC's action against Comcast on procedural grounds, prompting the FCC to initiate a formal rulemaking process to codify network neutrality principles in U.S. law.[47] The result was the 2010 Open Internet Order, a series of rules protecting lawful online content from blocking or unreasonable discrimination.[48] A federal court vacated most of the 2010 rules in January 2014 in response to a lawsuit led by Verizon, one of the nation's largest telecommunications companies.[49] The court held that the FCC had based the order on insufficient legal authority, eliminating the United States' only legal protections for network neutrality.

The success of Verizon's lawsuit sparked a public campaign for new rules that lasted more than a year and drew support from President Barack Obama, members of Congress, technology companies, consumer advocates, and millions of Americans who contacted the FCC. In February 2015, the FCC approved a new Open Internet Order that many legal experts believe is based on stronger legal authority than the 2010 order.[50] The order prohibits blocking and unreasonable discrimination on both fixed and wireless networks, reflecting the growing importance of mobile broadband in the United States. However, several broadband companies and their trade associations are once again suing the FCC to overturn the rules.[51] As of May 2015, the lawsuit was pending in federal court and many technology companies and public interest groups had formally joined the case to oppose the lawsuit and defend the FCC's rules.

Although the U.S. Constitution includes core protections for freedom of the press, the U.S. government does bring some enforcement actions against whistleblowers and journalists that may lead to self-censorship. The Attorney General has said that the 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,"[52] but investigations and prosecutions of several other whistleblowers and journalists are ongoing. In addition to the ongoing WikiLeaks grand jury investigation, which targeted at least three journalists' Google email accounts and metadata,[53] reporters from several major media outlets have had their communications collected in pursuit of other whistleblower investigations. As part of one investigation, for example, Fox News correspondent James Rosen was listed as a co-conspirator, was the subject of a warrant for his personal emails, and

46 Federal Communications Commission, "Commission Orders Comcast to End Discriminatory Network Practices," August 1, 2008, http://bit.ly/1OhQ4wN.

47 Cecilia Kang, "Court rules for Comcast over FCC in 'net neutrality' case," *Washington Post*, April 7, 2010, http://wapo.st/1L1WYjS.

48 Federal Communications Commission, "Report and Order," GN Docket No. 09-1919, December 21, 2010, http://bit.ly/1OhQ4wN.

49 Edward Wyatt, "Rebuffing F.C.C. in 'Net Neutrality' Case, Court Allows Streaming Deals," *New York Times*, January 14, 2014, http://nyti.ms/1fuX0WV.

50 Federal Communications Commission, "Report and Order on Remand, Declaratory Ruling, and Order: In the Matter of Protecting and Promoting the Open Internet," GN Docket No. 14-28, February 26, 2015, http://bit.ly/1NOC8bv; Shuli Wang, "The FCC's Net Neutrality Rules on Protecting and Promoting Open Internet," ed. Yaping Zhang, *JOLT Digest*, *Harvard Journal of Law and Technology,* March 23, 2015, http://bit.ly/1Le1RtH.

51 Jim Puzzanghera, "Opponents of FCC's net neutrality rules ask court for partial stay," *LA Times*, May 13, 2015, http://lat.ms/1KW5gvC.

52 Sari Horowitz, "Justice is reviewing criminal cases that used surveillance evidence gathered under FISA," *Washington Post*, November 15, 2013, http://wapo.st/1jKgo5Z.

53 Nick Cumming-Bruce, "WikiLeaks Assails Google and the U.S.," *New York Times*, Jan. 26, 2015, http://nyti.ms/1MUi0n9.

had his phone calls and appointments with a State Department suspect monitored.[54] In a separate investigation, the Department of Justice obtained two months' worth of Associated Press journalists' phone records.[55] In July 2013, in response to serious concerns raised by these investigations, the Department of Justice tightened the rules governing when and how the government could access journalists' records in investigations to ensure journalists could no longer be listed as co-conspirators, and to make it more difficult to obtain journalists' records without advance notice.[56] In October 2014, Attorney General Eric Holder also acknowledged that the investigation into Rosen was his greatest regret.[57]

Until January 2015, James Risen, an investigative reporter with the *New York Times*, was involved in an investigation into a whistleblower who was a source of information for his 2006 book, *State of War*. At some point between 2008 and 2015, Risen's phone and email records were collected,[58] and he faced possible imprisonment for refusing to disclose the name of his source. In 2015, the government relented and announced that it would not force Risen to testify about his source.[59]

Despite some improved protections, journalists report that their ability to investigate and publish freely is chilled. Several recent studies have concluded that the aggressiveness with which the Department of Justice investigates leaks — as well as pervasive government surveillance programs such as those disclosed by Edward Snowden — causes journalists and writers to self-censor and raises concerns about whether they are able to protect the confidentiality of their sources.[60]

In January 2015, the free expression and literature advocacy group PEN America released the results of an updated survey showing that the NSA surveillance revelations and other government actions had resulted in increased self-censorship among writers. During the 2014 year, 42 percent of respondents reported having altered or avoided social media activities, 31 percent reported deliberately avoiding certain topics in phone or email conversations, and 34 percent reported avoiding writing or speaking about a particular topic.[61] Additionally, Human Rights Watch and the American Civil Liberties Union conducted a survey of journalists and lawyers revealing the degree to which 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

54 Anne E. Marrimow, "A rare peek into a Justice Department leak probe," *Washington Post*, May 19, 2013, http://wapo.st/1Z3Mqdp.

55 Sari Horwitz, "Under sweeping subpoenas, Justice Department obtained AP phone records in leak investigation," *Washington Post,* May 13, 2013, http://wapo.st/1NgFxSj.

56 Charlie Savage, "Holder Tightens Rules on Getting Reporters' Data," *New York Times*, July 12, 2013, http://nyti.ms/1QUpeIK; See also Department of Justice, *Department of Justice Report on Review of News Media Policies*, July 12, 2013, http://1.usa.gov/1iZTxTo.

57 David A. Graham, "Does Eric Holder Want to Prosecute Journalists or Not?" *The Atlantic*, Oct. 29, 2014, http://theatln.tc/1zKrTjR.

58 Charlie Savage, "U.S. Gathered Personal Data on Times Reporter in Case Against Ex-C.I.A. Agent," *New York Times*, Feb. 25, 2011, http://nyti.ms/1LtkrQi.

59 Matt Appuzzo, "Times Reporter Will Not Be Called to Testify in Leak Case," *New York Times*, Jan. 12, 2015, http://nyti.ms/1AVPPAY.

60 Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy,* 2014, http://bit.ly/1uz3CL1; PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers*, January 5, 2015, http://bit.ly/1VBgCYT; see also PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, November 2013, http://bit.ly/1rZ3LXt; and Jesse Holcomb, Amy Mitchell, and Kristen Purcell, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*, Pew Research Center, February 5, 2015, http://pewrsr.ch/1xqJh6i.

61 PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers.*

secure their communications with clients, particularly in cases with foreign governments or prosecutions that might spark an intelligence inquiry.[62]

New evidence suggests that even ordinary American citizens are changing their behavior because of extensive government surveillance. A March 2015 study by the Pew Research Center on Americans' privacy strategies post-Snowden noted that 30 percent of people surveyed had altered their behavior including changing privacy settings, being more selective about applications they use, or communicating in person instead of online or over the phone.[63]

Digital Activism

Political activity in the United States is increasingly moving online. According to a 2014 survey by the Pew Research Center, between the 2010 and 2014 midterm elections, the proportion of Americans using social media to follow politicians more than doubled, from 6 percent to 16 percent.[64] In 2013, another Pew survey found that 34 percent of American adults used online methods to contact a government official or to speak out in a public forum; 39 percent participated in political activity using a social networking site like Facebook or Twitter in the prior year; and 21 percent of email users reported regularly receiving calls to action on social or political issues by email.[65] In addition, political candidates and elected officials increasingly use email, mobile apps, and online content to garner support and keep their constituents engaged. Researchers have come to a general consensus that internet use is now deeply linked to political participation and citizenship.[66]

An unprecedented number of Americans used online tools to mobilize in support of the open internet in 2014, resulting in the FCC's passage of a historic network neutrality order. Nearly 4 million Americans contacted the FCC about its proposed net neutrality rules — a record-breaking number that far exceeded the number of comments the agency had received on any topic in its history.[67] The FCC's website crashed several times as a result of the influx of public comments, notably after comedian John Oliver urged Americans to contact the agency in a televised rant that went viral on social networking websites.[68] A broad coalition of grassroots organizations, advocacy groups, and technology companies used online tools to mobilize supporters and pressure the FCC and elected officials. In September 2014, members of this coalition staged an "Internet Slowdown Day" in which dozens of high-profile websites displayed a spinning wheel to indicate what the internet could look like in a world without net neutrality protections.[69] When the FCC approved the strongest network neutrality rules in its history in February 2015, policymakers credited the millions of Americans who spoke out in online forums.[70]

62 Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy.*

63 Lee Rainieand and Mary Madden, *Americans' Privacy Strategies Post-Snowden*, Pew Research Center, March 16, 2015, http://pewrsr.ch/1MIHWjv.

64 Aaron Smith, *Cell Phones, Social Media, and Campaign 2014,* November 3, 2014, http://pewrsr.ch/1rTCqj1.

65 Aaron Smith, *Civic Engagement in the Digital Age*, Pew Research Center, April 25, 2013, http://pewrsr.ch/1nighxK.

66 Karen Mossberger et al., "Digital Citizenship: Broadband, Mobile Use, and Activities Online," (paper presented at Internation Political Science Association conference, Montreal, Canada, July 2014), http://paperroom.ipsa.org/papers/paper_36182.pdf.

67 Chris Welch, "FCC net neutrality debate passes Janet Jackson's nip slip in total comments," *The Verge*, September 10, 2014, http://bit.ly/1JOEbqg.

68 Soraya Nadia MacDonald, "John Oliver's net neutrality rant may have caused the FCC website to crash," *Washington Post*, June 4, 2014, http://wapo.st/1mzTd8j.

69 Barbara van Schewick, "Is the Internet about to get sloooooow?" *CNN*, September 10, 2014, http://cnn.it/1hlqw37.

70 Craig Aaron, "How We Won Net Neutrality," *The Blog, Huffington Post*, February 26, 2015, http://huff.to/18pvCYE.

Violations of User Rights

The United States has a robust legal framework that supports freedom of expression both online and offline, and the state 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.

Legal Environment

The First Amendment of the U.S. Constitution includes protections for free speech and freedom of the press, and in 1997 the US Supreme Court reaffirmed that online speech has the highest level of constitutional protection.[71] 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.[72]

There are some concerns, however, over conflicts about the right to remain anonymous in online communications, which often arise in cases of hate speech, defamation or libel. For example, in a recent case before the Supreme Court of Virginia, a judge ruled that a Virginia court could not compel Yelp to reveal the identities of anonymous users.[73]

Complementing these legal protections, a number of U.S. laws attempt to protect speech from harmful corporate actions as well, including corporate surveillance that may lead users to self-censor, and failure of private actors to sufficiently protect internet users' personal information from unauthorized access. Section 5 of the Federal Trade Commission Act (FTCA) has been interpreted to prohibit entities operating over the internet from deceiving users about what personal information is being collected and how it is being used, as well as from using personal information in ways that harm users without offering countervailing benefits. In addition, the FTCA has been interpreted to require entities that collect users' personal information to adopt reasonable security measures to safeguard it from unauthorized access. State-level laws in 47 U.S. states and the District of Columbia also require entities that collect personal information to notify consumers—and, usually, consumer protection agencies—when they suffer a security breach leading to unauthorized access of personal information. Section 222 of the Communications Act prohibits telecommunications carriers from

71 Reno, Attorney General of the United States, et al. vs. American Civil Liberties Union et al, 521 U.S. 844 (1997), http://bit.ly/1OT33VQ.

72 Center for Democracy and Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," April 2010, http://bit.ly/1hlr3Cj.

73 Justin Jouvenal, "Yelp won't have to turn over names of anonymous users after court ruling" *Washington Post,* 16 April 2015, http://wapo.st/1MbcE48.

sharing or using information about their customers' use of the service for other purposes without customer consent. This provision has historically only applied to phone companies' records about phone customers, but following the FCC's net neutrality order, it now also applies to ISPs' records about broadband customers.

Prosecutions and Detentions for Online Activities

- In the aftermath of the police killings of Eric Garner, Freddie Gray, and Michael Brown in New York, Baltimore, and Ferguson respectively, several citizen journalists were arrested or reported police intimidation while attempting to record police activity with smartphones. The right of civilians to film or record the police is protected under the First Amendment;[74] however, during the Ferguson protests at least 21 journalists were arrested, including reporters for the *Huffington Post* and the *Washington Post*. In addition, St. Louis Alderman Antonio French was detained by the police while covering police activity through live-tweets; French had also been uploading short videos and images to the social media platforms Vine and Instagram.

- 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.[75] 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.[76] 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 violations and stop prosecutors from bringing multiple redundant charges for a single crime.[77] The bill was reintroduced in 2015,[78] but has not garnered enough support to move forward. Meanwhile and in contrast to Aaron's Law, the Obama Administration—rather than supporting CFAA reform—has instead proposed draft legislation that would broaden the scope of activities covered under CFAA and make its penalties even harsher.[79]

- Many states also have their own laws related to computer hacking or unauthorized access. Several smaller cases in the past year highlight the shortcomings and lack of proportionality of these laws. In December 2014, a 21-year-old Georgia Tech student named Ryan Gregory Pickren was arrested on felony computer trespass charges after hacking into the University of Georgia's online calendar as part of a prank leading up to a football game. The prank calendar post, which was titled "Get Ass Kicked by GT," was live for approximately an hour

74 PEN America, *Press Freedom Under Fire in Ferguson*, October 27, 2014, http://bit.ly/1zDIsOl.

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

76 "Deadly Silence: Aaron Swartz and MIT," *The Economist*, August 3, 2013, http://econ.st/1L21COJ.

77 Representative Zoe Lofgren, official website, "Rep Zoe Lofgren Introduces Bipartisan Aaron's Law," press release, June 20, 2013, http://1.usa.gov/1QUsnbx.

78 Kaveh Waddell, "'Aaron's Law' Reintroduced as Lawmakers Wrestle Over Hacking Penalties," *National Journal*, April 21, 2015, http://bit.ly/1Pf4m0u.

79 Dana Liebelson, "Democrats, Tech Experts Slam Obama's Anti-Hacking Proposal," *Huffington Post*, January 20, 2015, http://huff.to/1hlrDzO.

before it was discovered and removed. However, according to Georgia state law, a person convicted for computer trespass—defined as "alter[ing], damag[ing] or in any way caus[ing] the malfunction of a computer, computer network, or computer program regardless of how long it occurs"—faces a maximum penalty of 15 years in prison and a $50,000 fine.[80] Pickren was ultimately accepted into a pretrial intervention program, and his charges will be dismissed upon his satisfactory completion. Similarly, in early 2015, Florida authorities arrested a 14-year-old middle school student named Domanik Green on felony cybercrime charges after the boy used a teacher's administrative password to log onto a school computer and change its desktop background.[81]

Surveillance, Privacy, and Anonymity

Concerns over government surveillance have grown since Edward Snowden's June 2013 revelations about NSA access to domestic and foreign communications. In response, Congress has put forth multiple legislative proposals to restrict, or in some cases maintain, NSA surveillance capabilities over the past two years. In January 2014, President Obama announced that he intended to end the bulk collection of telephony metadata.[82] In January 2015, the president also issued updates to the administration's 2014 policy directive that put in place important new restrictions on the use of information collected in bulk for foreign intelligence purposes.[83]

Additionally, in December 2014, Congress passed a bill that included a requirement that the NSA develop "procedures for the retention of incidentally acquired communications" collected pursuant to Executive Order 12333, and that, except when subject to certain broad exceptions, those communications may not be retained for more than five years.[84] This is the first time that Congress has legislated on executive activities under Executive Order 12333.

In June 2015, Congress passed the USA FREEDOM Act to extend expiring provisions of the PATRIOT Act, but with significant reforms to PATRIOT Act Section 215, as well as to the FISA Pen Register and Trap and Trace Device and National Security Letters authorities, both of which were also used for bulk or large-scale collection of Americans' information. The USA FREEDOM Act was broadly supported by the Attorney General, the Director of National Intelligence, Democrats and Republicans in Congress, as well as civil society and the private sector. Despite this broad support, it took several months to pass the act, and the final version embodied weaker reforms than what was advocated for by many supporters of surveillance reform. Owing to the difficulty of getting reform through Congress, reauthorization did not occur before a number of PATRIOT Act provisions expired on June 1, 2015.[85] After a single day lapse in surveillance authority, Congress finally passed the USA FREEDOM

80 Joe Johnson, "Georgia Tech student who hacked into UGA computer network gets pretrial diversion," *Athens Banner-Herald*, February 26, 2015, http://bit.ly/1FSEllk.

81 Josh Solomon, "Middle school student charged with cybercrime in Holiday," *Tampa Bay Times*, April 9, 2015, http://bit.ly/1ybpTBg.

82 The White House, Office of the Press Secretary, "Remarks by the President on Review of Signals Intelligence," January 17, 2014, http://1.usa.gov/1L0eJTT; The White House, Office of the Press Secretary, "FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program," March 27, 2014, http://1.usa.gov/1hls6lz.

83 Presidential Policy Directive – Signals Intelligence Activities PPD-28, January 17, 2014, http://1.usa.gov/1MUm5Yz.

84 H.R. 4681, Intelligence Authorization Act for Fiscal Year 2015 Sec. 309, 113th Cong. (2014).

85 New America Open Technology Institute, "Midnight Expiration of USA PATRIOT Act Adds New Pressure for Surveillance Reform: OTI Calls on Senate to Pass USA FREEDOM Act As Soon as Possible," press release, June 1, 2015, http://bit.ly/1WIqmD6.

Act, and President Obama signed it into law the same night.[86] The USA FREEDOM Act marks the most significant reforms to U.S. surveillance law since the PATRIOT Act passed in 2001.

Prior to the passage of the USA FREEDOM Act, as Congress was still debating legislative reforms, the courts considered three cases challenging the legality and constitutionality of the NSA's bulk collection program under PATRIOT ACT Section 215. In May 2015, the Second Circuit Court of Appeals ruled that the program was illegal, and that the government's interpretation of the term "relevance" exceeded what was authorized by statute. The court did not comment on the constitutional questions raised by bulk collection.[87] Two other cases are still pending, and the issue may eventually be taken up by the Supreme Court.

Finally, in April 2015, it was revealed that since the 1980s, the Department of Justice and the Drug Enforcement Agency had been collecting Americans' phone record metadata in bulk, amassing billions of records, apparently using the same interpretation of the term "relevance" that was the basis for the bulk collection program under PATRIOT Act Section 215. The program was stopped by Attorney General Eric Holder in September 2013, in response to the Snowden leaks which began earlier that summer.[88] Privacy, civil rights, and human rights organizations have spoken out in strong opposition to the program. The day the collection became public, Human Rights Watch filed a legal challenge to the program seeking that it be declared unlawful.[89]

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,[90] 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.[91] In April 2011, the Obama administration launched the National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to support 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 requiring assurance of identity.[92] The plan specifically endorses anonymous online speech.[93]

While there are no legal restrictions on anonymous communication online, there are 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. There is also evidence to suggest that the intelligence community

86 Kevin Bankston, "Senate Made History Today With Final Passage of USA FREEDOM Act: OTI Celebrates First Major Victory in Battle for Surveillance Reform," New America Open Technology Institute, June 2, 2015, http://bit.ly/1L24TO7.

87 Marty Lederman, "BREAKING: Second Circuit rules that Section 215 does not authorize telephony bulk collection program," Just Security, May 7, 2015, http://bit.ly/1j9kTqO.

88 Brad Heath, "U.S. secretly tracked billions of calls for decades," *USA Today*, April 8, 2015, http://usat.ly/1NS1eDA.

89 David Ingram, "Rights group sues DEA over bulk collection of phone records," *Reuters*, April 8, 2015, http://reut.rs/1E7A0bj.

90 Erica Newland, et. al., *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.

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

92 National Strategy for Trusted Identities in Cyberspace, "About NISTIC," accessed May, 14, 2014, http://1.usa.gov/1hluGbe.

93 Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" American Civil Liberties Union, January 7, 2011, http://bit.ly/1M7hILh; See also, Jim Dempsey, "New Urban Myth: The Internet ID Scare," *Policy Beta* (blog), Center for Democracy and Technology, January 11, 2011, http://bit.ly/1Oi3I2U.

in the United States has been working to undermine the security of anonymizing tools.[94] 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),[95] as well as efforts to undermine international technical standards for encryption.[96] Moreover, as major technology companies have begun enhancing their use of encryption technology in the past year, it has reignited a debate between law enforcement officials, technology experts, and privacy advocates about whether companies should be allowed to market products with strong encryption that do not preserve the government's ability to access decrypted versions of those encrypted communications.

In September 2014, Apple announced that it would be moving to smartphone encryption by default on all devices running its new iOS, followed a few days later by a similar announcement from Google about the latest version of the Android operating system.[97] In addition to advances in hardware encryption, a number of companies took greater steps to make end-to-end encryption available for email and messaging services, including the popular mobile messaging service Whatsapp and a joint Google-Yahoo effort to develop an easy-to-use encryption browser extension for their email services.[98] The added protection is, at least in part, a reaction to diminishing trust in American technology products following the 2013 Snowden leaks and increasing pressure from advocacy groups, individuals, and customers who are concerned about the security of their data.[99] In the year after the Snowden disclosures, encrypted web traffic doubled in North America.[100]

However, the Apple and Google announcements in particular have prompted serious backlash from the law enforcement and intelligence communities in the United States. The FBI Director has argued that Apple's and Google's new privacy-enhancing features will "allow people to place themselves beyond the law" and that default encryption could seriously hinder criminal investigations, calling on Congress to take action to force companies to maintain some kind of backdoor to allow government access to communications if a warrant has been obtained.[101] The Manhattan District Attorney called

94 For an in-depth discussion of NSA efforts to undermine Internet security, including attacks on Tor (a popular service used to anonymize web traffic) and attempts to undermine international encryption standards through the "Costs to Cybersecurity" in Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," New America's Open Technology Institute, July 2014, http://bit.ly/1GsrIbD.

95 James Ball, Bruce Schneier and Glenn Greenwald, "NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users," *The Guardian*, October 4, 2013, http://bit.ly/1cjtlsf.

96 James Ball, Julian Borger and Glenn Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian,* September 6, 2013, http://gu.com/p/3thvv/stw.

97 Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," *Washington Post*, September 18, 2014, http://wapo.st/1o4AjIx; Craig Timberg, "Newst Androids will join iPhones in offering default encryption, blocking police," *Washington Post*, September 18, 2014, http://wapo.st/1Vzlcfp.

98 Andy Greenberg, "Whatsapp Just Switched On End-to-End Encryption for Hundreds of Millions of Users," *Wired*, November 18, 2014, http://wrd.cm/1xTD5aY; Andrea Peterson, "Yahoo's plan to get Mail users to encrypt their e-mail: Make it simple," *Washington Post*, March 15, 2015, http://wapo.st/1Oi5Tn9.

99 Danielle Kehl and Kevin Bankston, "NSA Surveillance Costs and the Crypto Debate: Tech Companies Compete on Privacy Post-Snowden," New America's Open Technology Institute, October 17, 2014, http://bit.ly/1L294JC; See, e.g., the Electronic Frontier Foundation, *Encrypt the Web Report*, http://bit.ly/1r0ONPw; Access, "Encrypt All the Things" campaign, which promotes its "Data Security Action Plan," https://encryptallthethings.net/; and Fight for the Future, "Reset the Net" campaign, June 5, 2014, https://www.resetthenet.org/.

100 Doug Drinkwater, "Encrypted web traffic quadruples in Europe," *SC Magazine*, May 19, 2014, http://bit.ly/1QUznoL.

101 Craig Timberg and Greg Miller, "FBI blasts Apple, Google for locking police out of phones," *Washington Post*, September 25, 2014, http://wapo.st/1rg85As; "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?: A Conversation with FBI Director James Corney," The Brookings Institution video, October 16, 2015, http://brook.gs/1CqbsVT; David E. Sanger and Matt Apuzzo, "James Comey, FBI Director, Hints at Action as Cell Phone Data is Locked," *New York Times*, October 16, 2014, http://nyti.ms/1WIxJKH; "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, http://bit.ly/19mt79c.

device encryption a threat to public safety, while the former Attorney General urged tech companies to leave backdoors open for police.[102] Their arguments have received support from the National Security Agency and the Office of the Director for National Intelligence as well.[103] In the subsequent months, there has been a great deal of debate about the technical feasibility of implementing surveillance backdoors without undermining the overall security of cryptographic systems.[104]

On the other side of the spectrum, there have been efforts to codify rules that would *bar* the government from requiring surveillance backdoors. In the summer of 2014, the U.S. House of Representatives approved, with overwhelming bipartisan support, an appropriations amendment to ban spending on government-mandated backdoors, although procedural maneuvers prevented it from being adopted into the final bill.[105] In the summer of 2015, the House again approved two similar amendments.[106] Building on that support, the Secure Data Act was introduced in Congress in December 2014, which would similarly prohibit the government from requiring that companies weaken the security of their products or insert backdoors to facilitate access.[107]

Despite a vigorous debate, there have been no actual changes on the legislative front regarding the use of encryption, nor is there any indication that the government is currently planning to move forward with the technical solutions it has proposed.[108] While the Communications Assistance for Law Enforcement Act (CALEA) currently 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, it does not cover online communications tools such as Gmail, Skype, and Facebook.[109] Calls to update CALEA to cover online applications and communications have not been successful. 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.[110]

102 Cyrus R. Vance Jr., "Apple and Google threaten public safety with default smartphone encryption," *Washington Post*, September 26, 2014, http://wapo.st/1hlxC7Y; Craig Timberg, "Holder urges tech companies to leave device backdoors open for police," *Washington Post*, September 30, 2014, http://wapo.st/1Oi7idn.

103 Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *Washington Post*, April 10, 2015, accessed May 21, 2015 http://wapo.st/1KB3ZsB; "VIDEO: ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," Office of the Director of National Intelligence: IC on the Record video, 1:26:28, February 4, 2015, http://bit.ly/1VzmJCn.

104 Bruce Schneier, "Stop the hysteria over Apple encryption," *CNN*, October 31, 2014, http://cnn.it/1sSk7RX; Joseph Lorenzo Hall, "The NSA's Split-Key Encryption Proposal is Not Serious," Center for Democracy & Technology, April 20, 2015, http://bit.ly/1M7nYm8; Julian Sanchez, "What NSA Director Mike Rogers Doesn't Get About Encryption," Cato Institute, February 24, 2015, http://bit.ly/17UaGYN.

105 See Amendment to H.R. 4870, the Department of Defense Appropriations Act, offered by Representative Massie of Connecticut. The Amendment "prohibits funds for the government to request that products or services support lawful electronic surveillance": The FY 2015 Department of Defense Appropriations Bill: House Adopted Amendments, H.R. 4870 (2014), http://1.usa.gov/1jDUJpd.

106 Robyn Greene, "Representatives Should Vote "Yes" on Three Amendments to Prohibit Bulk Collection and to Protect Encryption," New America Open Technology Institute, June 2, 2015 [updated June 3, 2015], http://bit.ly/1M7pLHQ.

107 Secure Data Act of 2014, S.2981, 113th Cong. (2014), http://1.usa.gov/1Lc1Eme. The bill was reintroduced in 2015, although no further action has been taken.

108 Cory Bennett, "Lawmakers skeptical of FBI's encryption warnings," *The Hill*, April 29, 2015, http://bit.ly/1bGPbwO.

109 Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet." *New York Times*, September 27, 2010, http://nyti.ms/1WIzNlX; See also Declan McCullagh, "FBI: We Need Wiretap-Ready Websites – Now," *CNET*, May 4, 2012, http://cnet.co/1iRh6vA.

110 Ben Adida et al, *CALEA II: Risks of Wiretap Modifications to Endpoints*, Center for Democracy & Technology, May 17, 2013, http://bit.ly/1Gsv12v.

Since the June 2013 surveillance revelations, internet and telecommunications companies have increasingly taken up the practice of "transparency reporting" in an effort to shed light on the government's surveillance powers and how the companies handle requests. Transparency reports, which are voluntarily published, detail requests for government access to user information, user communications, and/or requests to have content removed or filtered. One limit to the reporting, however, has been the U.S. Department of Justice's restrictions on disclosure of information about national security orders.[111] In October 2014, Twitter filed suit against the DOJ, arguing that the government's restrictions on what information companies can disclose about national security letters are unconstitutional.[112] Earlier in 2014, the Justice Department had reached a settlement with Facebook, Google, LinkedIn, Microsoft, and Yahoo that would permit the companies to disclose the number of government requests they receive – but only in aggregated bands of 0-249 or 0-999.[113] Twitter, not a party to the settlement, has refused to publish data in these aggregated bands because the company believes the DOJ rules amount to an unconstitutional prior restraint that violates the company's First Amendment rights.[114] The DOJ has called for dismissal of the lawsuit.[115] A large and wide-ranging group of internet and telecommunications companies, including Wikipedia and Automattic (publisher of Wordpress.com), have shown support for Twitter's challenge to the DOJ rules by filing briefs in court in support of Twitter.[116]

The U.S. District Court for the Northern District of California may no longer proceed with the lawsuit, however, given new legal processes implemented by the USA FREEDOM Act.[117] Under the new law, companies now have several options on how to report the number and nature of national security orders and other government requests, and can also do so in a more granular fashion than was previously permitted. Yet, depending on the option, these reports are still subject to time delays and have limitations on the frequency of reporting.[118]

In addition to monitoring private communications, law enforcement agencies have also used open, public websites and social media platforms to monitor different groups for suspected criminal activity. The New York Police Department (NYPD) is one such agency, with the Associated Press reporting that, from 2006 onward, the NYPD Cyber Intelligence unit 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.[119] 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,

111 Craig Timberg & Adam Goldman, "U.S. to Allow Companies to Disclose More Details on Government Requests for Data," *Washington Post,* January 27, 2014, http://wapo.st/LhuLxw.

112 Alexei Oreskovic, "Twitter Sues U.S. Justice Department for Right to Reveal Surveillance Requests," *Reuters,* October 7, 2014, http://reut.rs/1yLKbRe.

113 Office of the Deputy Attorney General, email correspondence fto Facebook, Google, LinkedIn, Microsoft, and Yahoo general counsels, January 27, 2014, http://1.usa.gov/1IuJYqL.

114 Ben Lee, "Taking the fight for #transparency to court," *Twitter Blog*, October 7, 2014, http://bit.ly/Zc3Mtm.

115 Ellen Nakashima, "Justice Department Seeks to Dismiss Most of Twitter's First Amendment Lawsuit," *Washington Post*, January 20, 2015, http://wapo.st/1Og5VKH.

116 Jeff Roberts, "Tech and Media Firms Join Twitter in Key Test of FBI Gag Orders," Gigaom Research, February 18, 2015, http://bit.ly/1Gsvi5J.

117 Dan Levine, "UPDATE 1-Judge casts doubt on Twitter lawsuit over surveillance," *Reuters*, June 11, 2015, http://reut.rs/1VBu4Mj.

118 For additional information on reporting standards, please reference: USA Freedom Act, H.R. 2048 (2015), http://1.usa.gov/1jKsHzc.

119 Associated Press,"AP's Probe Into NYPD Intelligence Operations," accessed May 5, 2015 http://bit.ly/L3pdWB.

including mosques and businesses.[120] Civil liberties advocates welcomed this step but warned that other NYPD units may still be using discriminatory practices.

Federal intelligence agencies closely monitor social media as part of their terrorism investigations.[121] This monitoring leads to the identification of specific targets, who are then contacted by FBI informants. This was the case in the January 2014 arrest of an Ohio man whose posts on Twitter first drew the attention of the FBI and who was ultimately arrested for planning to attack the Capitol.[122] While monitoring open, public websites and social media platforms has yielded some arrests, it is not limited to targets of investigations, but rather is used to identify targets, and includes monitoring of innocent individuals' online activities. Thus, it may chill online speech.

In comparison to real-time communications, 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.[123] However, the 1986 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.[124] Bills to update ECPA have had significant support, including from the White House, but have thus far failed to pass. As of mid-2015, 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 services.[125]

Intimidation and Violence

In addition to arrests and detentions for filming police activities, individuals have been subject to intimidation and harassment. Kevin Moore, the man who used his cellphone to capture and upload footage of Freddie Gray's arrest by the Baltimore police to YouTube, was also detained by the police after releasing the video. Additionally, Moore claims he was followed by the police and experienced other forms of intimidation.[126] Similarly, Ramsey Orta, the man who filmed the fatal arrest of Eric Garner by the NYPD—footage in which Garner repeatedly states "I can't breathe" after being placed in a chokehold—also claims to have been repeatedly followed, harassed, and intimidated by the police after his role in documenting the killing. Since the footage was released, the 23-year old Orta has been arrested on three separate occasions and currently awaits trial for multiple charges.[127]

Technical Attacks

120 Matt Appuzzo and Joseph Goldstein, "NY Drops Unit that Spied on Muslims," *New York Times*, Apr. 15, 2014, http://nyti.ms/1evekec.

121 Kevin Sullivan, "Three American teens, recruited online, are caught trying to join the Islamic State," *Washington Post*, December 8, 2014, http://wapo.st/1L2hEIz.

122 Sari Horwitz, "Ohio man arrested in alleged plot to attack Capitol," *Washington Post*, January 14, 2015, http://wapo.st/1Rr8cml.

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

124 Ibid.

125 Greg Nojeim, "Senate 'Dream Team' Introduced ECPA Reform Bill," *Beta Policy Blog*, Center for Democracy and Technology, March 19, 2013, http://bit.ly/1j9sRQE; See also Digital Due Process, "ECPA: About the Issue," accessed April 23, 2013, http://bit.ly/1d1VVAr.

126 Mariah Stewart, "Man Who Filmed Freddie Gray Arrest Detained By Baltimore Police, Along With Ferguson Video Activists," *Huffington Post*, http://huff.to/1VBuAtR.

127 Josh Sanbur, "The Witness," *Time*, http://time.com/ramsey-orta-eric-garner-video/.

Financial, commercial, and governmental entities in the United States are targets of significant cyberattacks. Government policies and laws are in place to prevent and protect against cyberattacks, though many question their impact, effectiveness, and respect for civil liberties.

In August 2014, reports revealed that JPMorgan Chase and several other major U.S. financial institutions were hit with a cyberattack that "funneled off gigabytes of data."[128] Similar attacks were carried out against the retailers eBay and Home Depot in 2014. In addition to the attacks resulting in data theft, U.S. banks fell victim to the "Carbanak" cyber-heist that siphoned nearly $1 billion from financial institutions since 2013.[129] Finally a high-profile attack on Sony Pictures Entertainment's internal networks extracted private data and leaked it to the public. The attack on Sony Pictures was likely politically driven, as the attackers attempted to blackmail the company with the stolen data to prevent it from releasing a controversial comedy about North Korea.

Financial and commercial institutions are not the only U.S. institutions subject to cyberattacks. Health information has been the target of a number of high profile attacks, and a reported 90 percent of healthcare providers experienced a breach in the past two years.[130] The motive for breaches of health records is usually financial, as those records can in turn be used to facilitate medical identity theft.[131] There has been some speculation that some of these attacks may be the work of foreign state-sponsored hackers looking to uncover information about defense contractors, government employees, and others with close ties to the U.S. government.[132]

The defense sector and federal government are also frequently under attack. In April 2015, the public learned that Russian hackers had breached the White House's system, accessing the email archives of President Obama and other sensitive information, including real-time, non-public details of the president's schedule.[133] In June 2015, news broke that hackers had breached the U.S. Office of Personnel Management's records system, affecting the records of 4.1 million current and former federal employees. The breach was linked to a Chinese state-backed hacker known as "Deep Panda."[134] In response to these incidents and others, the U.S. has begun to take legal and policy measures to address growing cyber-threats.

In particular, the U.S. Congress has been attempting to pass a law to facilitate greater sharing of information about cyber-threats. As of June 2015, Congress was considering the Cyber Information Sharing Act of 2015 (CISA). Civil liberties advocates have heavily criticized the bill, in particular contending that it authorizes too much information sharing between companies and the government, allows companies to monitor all of their users' activities and communications, does not adequately restrict use of CISA-derived information, has poor liability protections for consumers, and authoriz-

128 Laura Lorenzetti, "JPMorgan Chase, other U.S. banks hit by cyberattacks," *Fortune*, August 28, 2014, http://for.tn/1j0scQV.

129 Virus News,"The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide," Kaspersky Lab, February 16, 2015, http://bit.ly/1L5dnWl.

130 Shannon Pettypiece, "Rising Cyber Attacks Costing Health System $6 Billion Annually," *Bloomberg Business*, May 7, 2015, http://bloom.bg/1JtqQpr.

131 Ponemon Institute, "2014 Fifth Annual Study on Medical Identity Theft," 8, http://bit.ly/1JD1OIu; Dan Munro, "New Study Says Over 2 Million Americans Are Victims Of Medical Identity Theft," *Forbes*, February 23, 2015, http://onforb.es/1D3oNn8.

132 Michael A. Riley and Jordan Robertson, "Chinese State-Sponsored Hackers Suspected in Anthem Attack," *Bloomberg Business*, February 5, 2015, http://bloom.bg/1AwKK24.

133 Evan Perez and Shimon Prokupecz, "How the US thinks Russians Hacked the White House," *CNN*, April 8, 2015, http://cnn.it/1DiykuU.

134 David Perera, "Researchers: 'Deep Panda' Behind Hacking of Federal Data," *Politico*, June 4, 2015, http://politi.co/1OgcZad.

es companies to employ potentially dangerous counter-measures when hacked.[135] As of June 2015, Congress was also considering a number of legislative proposals to mandate security protections for personal information held by private entities.

In addition to the legislative activity, President Obama has issued two Executive Orders aimed at addressing cyberattacks. In January 2015, in response to the Sony Pictures hack, Obama issued an order authorizing the Treasury Department to impose sanctions on individuals and entities associated with the North Korean government.[136] Then, in April, the White House issued an Executive Order permitting the U.S. Department of the Treasury to levy sanctions against individuals or companies that conduct "significant malicious cyber-enabled activities."[137]

Law enforcement has also played a role in creating a framework to deter cyberattacks. In May 2014, the Western District of Pennsylvania indicted six officers in Unit 61398 of the Third Department of China's People's Liberation Army (PLA), alleging economic espionage against a number of U.S. based companies.[138] In July 2014, the Department of Justice announced that it charged Su Bin, a Chinese businessman, with hacking the computers of "Boeing, Lockheed Martin, and other aerospace companies" with the intent to gather data on the F-22, F-35, and C-17 aircrafts.[139]

135 Robyn Greene, "Cybersecurity Information Sharing Act of 2015 is Cyber-Surveillance, Not Cybersecurity," New America Open Technology Institute, April 9, 2015, http://bit.ly/1WIGSD4.

136 Zeke J. Miller, "U.S. Sanctions North Korea Over Sony Hack," *Time*, January 2, 2015, http://ti.me/1JP4EnL.

137 , The White House, Office of the Press Secretary, "Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015, http://1.usa.gov/1F2sjPD.

138 Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014, http://1.usa.gov/1pySTOP.

139 Sean Gallagher, "Chinese businessman charged with hacking Boeing, Lockheed Martin", *Ars Technica*, July 13, 2014, http://bit.ly/1rvJk0y.