Freedom House

# United States

| | 2016 | 2017 |
|---|---|---|
| **Internet Freedom Status** | **Free** | **Free** |
| Obstacles to Access (0-25) | 3 | 3 |
| Limits on Content (0-35) | 2 | 4 |
| Violations of User Rights (0-40) | 13 | 14 |
| **TOTAL* (0-100)** | **18** | **21** |

* 0=most free, 100=least free

| | |
|---|---|
| **Population:** | **323.1 million** |
| **Internet Penetration 2016 (ITU):** | **76.2 percent** |
| **Social Media/ICT Apps Blocked:** | **No** |
| **Political/Social Content Blocked:** | **No** |
| **Bloggers/ICT Users Arrested:** | **No** |
| **Press Freedom 2017 Status:** | **Free** |

## Key Developments: June 2016 – May 2017

- Social media were flooded with hyperpartisan and fake content during the 2016 presidential election campaign. Russian-operated social media accounts and state media engaged in disinformation and influence campaigns to polarize the media environment (see "**Media, Diversity, and Content Manipulation**").
- Americans witnessed several major cyberattacks in the latter half of 2016, including the hacking and subsequent leaking of sensitive information from the Democratic National Committee in the lead-up to the vote (see "**Technical Attacks**").
- Journalists writing about political or social topics faced an uptick in antisemitism, death threats, and harassment on social media in the lead-up to the election (see "**Intimidation and Violence**").
- In April 2017, the NSA announced that it would halt a practice known as "about surveillance," which is authorized under Section 702 of the FISA Amendments Act and had resulted in the incidental collection of Americans' communications that contained references to a foreign surveillance target (see "**Surveillance, Privacy, and Anonymity**").
- Under new leadership, the Federal Communications Commission announced its intention to roll back net neutrality protections contained in the Open Internet Order passed in 2015 (see "**Regulatory Bodies**").

# Introduction

Pervasive disinformation and hyperpartisan content had a significant impact on internet freedom in the United States over the past year. In addition, journalists faced increased threats and harassment on online platforms.

As the U.S. presidential election dominated mainstream media coverage and social media conversations, groups seeking to sow doubt through disinformation, conspiracy theories, and hyperpartisan messaging took advantage of the news media environment.[1] While fake news existed on all parts of the political spectrum, the most popular stories predominantly favored candidate Donald Trump over Hillary Clinton. In January 2017, U.S. intelligence agencies concluded that Russia had interfered in the election do "denigrate Secretary Clinton" and "undermine public faith in the U.S. democratic process."[2] The agencies also assessed that Russian intelligence services had hacked into the servers of prominent U.S. political organizations and subsequently released leaked information to third parties. Testifying before Congress in October 2017, a representative from Facebook estimated that accounts associated with the Internet Research Agency (IRA), a "troll farm" based in Saint Petersburg, Russia, shared 80,000 posts on its platform between June 2015 and August 2017 that, when reposted by others, reached some 126 million American users. The IRA spent around $100,000 to amplify the visibility of their posts, which consisted of "divisive social and political messages across the ideological spectrum."[3] According to Twitter, over 36,000 Russia-linked automated accounts posted 1.4 million election-related tweets, receiving 288 million views from September 1 to November 15, 2016. The company noted these tweets represented less than one percent of all election-related tweets on the platform during that period.[4]

In a heightened climate of hostility towards critical news reporting, journalists also received threatening and antisemitic messages on social media.[5] During the campaign and once in office, the Trump administration continued to disparage journalists using derogatory or threatening language, and has denied journalists from both traditional and online media outlets from covering certain events or attending press briefings.

Following the U.S. presidential election, the leadership of the Federal Communications Commission switched parties, and President Trump appointed Republican commissioner Ajit Pai as the new FCC chairman. In the first few months of his leadership, Pai indicated his intention to deregulate the telecommunications industry and potentially reverse net neutrality protections. On April 27, 2017, the FCC issued a notice of proposed rulemaking (NPRM) seeking to remove the Title II classification for broadband service providers that had allowed the FCC to regulate broadband as a utility.[6] Pai

1 Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," Data and Society Research Institute, May 2017, https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

2 Scott Shane, "What Intelligence Agencies Concluded About the Russian Attack on the U.S. Election," *The New York Times*, January 6, 2017, https://www.nytimes.com/2017/01/06/us/politics/russian-hack-report.html?_r=0

3 Committee on the Judiciary, "Hearing before the United States Senate Committee on the Judiciary Subcommittee on Crime and Terrorism: Testimony of Colin Stretch," October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf

4 Sean Edgett, "U.S. Senate Committee on the Judiciary: Opening Remarks," Twitter Blog, October 31, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/opening_remarks.html

5 https://www.adl.org/sites/default/files/documents/assets/pdf/press-center/CR_4862_Journalism-Task-Force_v2.pdf

6 Federal Communications Commission, "Fact Sheet: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108," April 28, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

has suggested that the industry should regulate itself instead.[7] The FCC extended the deadline for accepting public comments on the proposal through August 30.[8][9]

On a positive note, the NSA announced in April 2017 that it would stop the practice of collecting U.S. citizens' emails that contain references to foreign targets of surveillance.[10] This practice, part of what is known as "upstream" collection, had resulted in the collection of Americans' emails for simply mentioning a foreign surveillance target, as opposed to communications sent to or received from a target. Privacy advocates welcomed the change in policy, but noted that the case highlights the need for legislative reform of Section 702 of the FISA Amendments Act, which authorized the "upstream" collection in the first place.

## 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 warn that insufficient competition in the ISP market could increase the cost of access. Under new leadership, the FCC has signalled its intention to deregulate the telecommunications industry and potentially reverse the net neutrality provisions the FCC enacted in 2015 with the Open Internet Order.*

### Availability and Ease of Access

| Key Access Indicators | | |
|---|---|---|
| Internet penetration (ITU)[a] | 2016 | 76.2% |
| | 2015 | 74.6% |
| | 2011 | 69.7% |
| Mobile penetration (ITU)[b] | 2016 | 127% |
| | 2015 | 118% |
| | 2011 | 94% |
| Average connection speeds (Akamai)[c] | 2017(Q1) | 18.7 Mbps |
| | 2016(Q1) | 15.3 Mbps |

[a] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," http://bit.ly/1cblxxY.
[b] International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2016," http://bit.ly/1cblxxY.
[c] Akamai, "State of the Internet - Connectivity Report, Q1 2017," https://goo.gl/TQH7L7.

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 76 percent by the end of 2016.[11] Broadband adoption rates are high: nearly

7 Cecilia Kang, "FCC Chairman Pushes Sweeping Changes to Net Neutrality Rules," *New York Times*, April 26, 2017, https://www.nytimes.com/2017/04/26/technology/net-neutrality.html?_r=0

8 Federal Communications Commission, "Fact Sheet: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108," April 28, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

9 Lauren Gambino and Dominic Rushe, "FCC flooded with comments before critical net neutrality vote," *The Guardian*, August 30, 2017, https://www.theguardian.com/technology/2017/aug/30/fcc-net-neutrality-vote-open-internet

10 Charlie Savage, "N.S.A Halts Collection of Americans' Emails about Foreign Targets," *New York Times*, April 28, 2017, https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html

11 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," http://bit.ly/1FDwW9w

three quarters (73 percent) of Americans report having broadband access at home as of November 2016.[12] While the broadband penetration rate is high by global standards, it lags significantly behind countries such as Switzerland, the Netherlands, Denmark, and South Korea.[13] Moreover, access, cost, and usability remain barriers for some Americans, particularly senior citizens, people who live in rural areas, and low-income households.[14] However, internet access rates for those 65 years of age and older has steadily increased over the past decade, with 64 percent of individuals in this age bracket using the internet as of 2016, according to data from Pew Research.[15]

In January 2015, citing advances in technology, market offerings, and consumer demand, the Federal Communications Commission (FCC) updated its benchmark speeds for broadband internet service to 25 Megabits per second (Mbps) download and 3 Mbps upload, up from the 2010 standard of 4 Mbps download and 1 Mbps upload. Under the new definition, the FCC found that 10 percent of the population lacks access to broadband service in its January 2016 report, compared to 17 percent in 2015.[16]

The cost of broadband internet access in the United States continues to be higher than many countries in Europe with similar internet penetration rates.[17] In March 2016, the FCC announced plans to expand its Lifeline program, which allows companies to offer subsidized phone plans to low income households, to include broadband internet access as a subsidized utility.[18] However, the current FCC administration delayed this expansion in February 2017, stating that it first needed to address issues of fraud.[19]

Uptake rates for internet-enabled mobile devices have increased dramatically throughout the United States in recent years. In 2016, 95 percent of adults reported that they owned a mobile phone, and 77 percent of adults owned a smartphone, up from 35 percent in 2011.[20] A growing number of people used their cell phones to view streaming video services offered by companies such as Netflix or Hulu (33 percent of smartphone owners in 2015, compared to 15 percent in 2012).[21] Pew Research reported in early 2015 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.[22]

12 Aaron Smith, "Record shares of Americans now own smartphones, have home broadband," Pew Research Center, January 12, 2017, http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

13 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."

14 Andrew Perrin, "Digital gap between rural and nonrural Americans persists," Pew Research Center, May 19, 2017, http://www.pewresearch.org/fact-tank/2017/05/19/digital-gap-between-rural-and-nonrural-america-persists/

15 "Internet Broadband Factsheet," Pew Research Center, January 12, 2017, http://www.pewinternet.org/fact-sheet/internet-broadband/

16 Federal Communications Commission, "2016 Broadband Progress Report," Federal Communications Commission, January 29, 2016, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report

17 "The Cost of Connectivity 2014," Open Technology Institute, October 30, 2014, https://www.newamerica.org/oti/policy-papers/the-cost-of-connectivity-2014/

18 John D. McKinnon, "Phone Subsidy for Poor Could Expand to Include Broadband," *Wall Street Journal*, March 8, 2016, https://www.wsj.com/articles/phone-subsidy-for-poor-could-expand-to-include-broadband-1457460517

19 Jacob Kastrenakes, "FCC slows expansion of low-income broadband subsidies," *The Verge*, February 3, 2017, https://www.theverge.com/2017/2/3/14503746/fcc-lifeline-erate-actions-reversed

20 "Mobile Fact Sheet," Pew Research Center, January 12, 2017, http://www.pewinternet.org/fact-sheet/mobile/

21 Monica Anderson, "More Americans using smartphones for getting directions, streaming TV," Pew Research Center, January 29, 2016, http://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use/

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

## 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 telecommunications companies, 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 in emergency situations. The federal government has a secret protocol for shutting down wireless internet connectivity in response to particular events, some details of which came to light following a lawsuit brought under the Freedom of Information Act.[23] The protocol, known as Standard Operating Procedure (SOP) 303, was established in 2006 on the heels of a 2005 cellular-activated subway bombing in London and codifies the "shutdown and restoration process for use by commercial and private wireless networks during national crises." 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.[24]

State and local law enforcement also have tools to jam wireless internet.[25] 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.[26]

On October 20, 2016, the ACLU of North Dakota and the National Lawyers Guild filed Freedom of Information Act and North Dakota Open Records Act requests in an effort to determine whether state or federal agencies had engaged in the disruption of mobile networks during protests near the Standing Rock reservation in North Dakota.[27] Protestors demonstrating against the construction of the Dakota Access oil pipeline reported experiencing irregular behavior on their mobile phones, including phones inexplicably crashing or rapidly running out of battery, and problems uploading posts to Facebook or livestreaming.[28] Cell-site simulators, such as Stingrays, are predominantly used by law enforcement for surveillance purposes but have also been known to disrupt the mobile phone activity of any individuals in the area where they are used.[29] Without specific evidence of law enforcement actions, however, it is unknown whether these disruptions were due to government interference or other variables, such as an overloaded mobile network. The Electronic Frontier Foundation has submitted public records requests to federal, state, and local agencies. Those that

23 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

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

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

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

27 National Lawyers Guild, "NLG and ACLU Submit FOIA and Open Records Requests to Investigate Unconstitutional Surveillance of Water Protectors at Standing Rock," Press release, October 20, 2016, https://www.nlg.org/nlg-and-aclu-submit-foia-and-open-records-requests-to-investigate-unconstitutional-surveillance-of-water-protectors-at-standing-rock/.

28 Alyssa Newcomb, Daniel A. Medina, Emmanuelle Saliba, and Chiara Sottile, "At Dakota Pipeline, Protestors Questions of Surveillance and 'Jamming' Linger," NBC News, October 31, 2016, http://www.nbcnews.com/storyline/dakota-pipeline-protests/dakota-pipeline-protesters-questions-surveillance-jamming-linger-n675866.

29 Kim Zetter, "Feds Admit Stingrays Can Disrupt Cell Service of Bystanders," *Wired*, March 1, 2015, https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/.

had responded by mid-December have denied the use of cell-site simulators.[30]

## ICT Market

While there are many broadband service providers operating in the United States, the industry has trended toward consolidation. On May 6, 2016, the FCC announced that it had voted to approve Charter Communications Inc.'s acquisition of Time Warner Cable and Bright House Networks, which was subsequently approved by the California Public Utilities Commission.[31] As of mid-2016, two companies—Comcast and Charter Communications—controlled an estimated 70 percent of the market for fixed-line broadband internet access, with approximately 24 million and 22 million subscribers respectively.[32] AT&T is the third largest broadband provider with 15.6 million subscribers, followed by Verizon with 7 million and CenturyLink with 6 million.[33] 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.[34]

Further consolidation of the telecom sector threatens to limit consumer choice of ICT services. The FCC has made some attempts to mitigate these threats in recent merger approvals. For example, the FCC included provisions within the recent Charter-Time Warner Cable deal that required Charter Communications to expand broadband availability in an effort to close the digital divide, including establishing new cable lines in areas of California without access, and providing affordable internet access to at least 525,000 low-income families.[35] Other conditions prohibit the companies from taking steps that would privilege cable services over online video competitors, such as imposing data caps on online content that would discourage subscribers from streaming video.[36] In 2015, regulators had blocked a proposed merger between Time Warner Cable and Comcast, citing concerns about Comcast's ability to interfere with over-the-top services (such as Netflix), as well as increased market concentration.[37]

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 — which accounted for 98 percent of the market share by the end of 2014. Verizon leads the wireless services

30 Stephanie LaCambra, "Investigating Law Enforcement's Possible Use of Surveillance Technology at Standing Rock," Electronic Frontier Foundation, December 15, 2016, https://www.eff.org/deeplinks/2016/12/investigating-law-enforcements-use-technology-surveil-and-disrupt-nodapl-water

31 Meg Jones, "California regulators approve Charter's takeover of Time Warner Cable," *Los Angeles Times*, May 12, 2016, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-charter-puc-20160512-snap-story.html

32 Jon Brodkin, "Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions," ArsTechnica, January 26, 2016, http://arstechnica.com/business/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/

33 Jon Brodkin, "Cable expands broadband domination as AT&T and Verizon lose customers," *Ars Technica,* August 16, 2016, https://arstechnica.com/information-technology/2016/08/cable-expands-broadband-domination-as-att-and-verizon-lose-customers/

34 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

35 Meg Jones, "California regulators approve Charter's takeover of Time Warner Cable," *Los Angeles Times*, May 12, 2016, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-charter-puc-20160512-snap-story.html

36 Jon Brodkin, "Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions," ArsTechnica, January 26, 2016, http://arstechnica.com/business/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/

37 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

market with 143 million subscribers, followed by AT&T with 132 million, T-Mobile with 67 million, and Sprint with 58 million.[38] The U.S. government has looked unfavorably on further consolidation of mobile networks. Regulators blocked AT&T's proposed merger with T-Mobile in 2011, and separately signaled that they would block a rumored merger between Sprint and T-Mobile in 2014.[39] Moreover, the government has promoted mobile broadband through a series of spectrum auctions. In March 2016, the FCC began the process of buying back airwaves set aside for TV broadcasters to increase the available spectrum for wireless broadband, as outlined in the government's 2012 National Broadband Plan, which set a goal of establishing universal broadband by 2020.[40]

In January 2015, then-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.[41] One month later, the FCC "preempted," or overturned, state laws in Tennessee and North Carolina that restrict local broadband services, arguing that such laws create barriers to broadband deployment.[42] In August 2016, a federal court ruled that the FCC does not have the authority to preempt these state laws,[43] which are also on the books in many other states. Critics contend that the ruling threatens to limit affordable broadband options for small remote communities.

## 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 since February 2015, when it issued a decision to legally classify broadband as a telecommunications service under the Communications Act (although the current FCC is reconsidering this authority). 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.

Typically the FCC is led by five commissioners, nominated by the president and confirmed by the Senate, with no more than three commissioners from one party. President Donald Trump nominated

38 Mike Dano, "How Verizon, AT&T, T-Mobile, Sprint, and more stacked up in Q2 2016," Fierce Wireless, August 15, 2016, http://www.fiercewireless.com/wireless/how-verizon-at-t-t-mobile-sprint-and-more-stacked-up-q2-2016-top-7-carriers

39 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

40 Colin Lecher, "How the FCC's massive airways auction will change America—and your phone service," *The Verge*, April 21, 2016, http://www.theverge.com/2016/4/21/11481454/fcc-broadcast-incentive-auction-explained

41 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

42 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

43 See *State of TN vs. FCC*, http://www.ca6.uscourts.gov/case_reports/rptPendingAgency.pdf; Brian Fung, "Cities looking to compete with large Internet providers just suffered a big defeat," *Washington Post,* August 1-, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/08/10/the-government-just-lost-a-big-court-battle-over-public-internet-service/

Republican commissioner Ajit Pai to serve as chair on January 23, 2017.[44] The FCC had only three commissioners for the first half of 2017, but returned to its five-member makeup when the U.S. Senate voted on August 3 to confirm Democrat Jessica Rosenworcel and Republican Brendan Carr.[45]

Since assuming his role as chair of the Commission, Pai has taken a number of steps toward deregulating the telecommunications industry. On March 1, the Commission voted to freeze the broadband privacy guidelines that the FCC had passed the previous October.[46] The guidelines would have required broadband providers to obtain opt-in consent from consumers before they could use and share information such as a user's web browsing history and app usage data, and would have given consumers the ability to opt-out of the use and sharing of other types of personally identifiable information.[47] In late March, Congress went a step further and voted to repeal the broadband privacy guidelines under the Congressional Review Act,[48] which effectively prevents the FCC from enacting similar rules in the future.[49]

On April 27, 2017, the FCC issued a notice of proposed rulemaking (NPRM – a tool used by independent government agencies to indicate a proposed change to a rule or law) that signaled the FCC's intention to deregulate the telecommunications industry and potentially reverse the net neutrality provisions the FCC enacted in 2015 with the Open Internet Order.[50] The Open Internet Order reclassified broadband internet providers as common carriers under Title II of the Communications Act, paving the way for the FCC to regulate ISPs as they do public utilities. The Open Internet Order also stipulated that broadband providers refrain from blocking or throttling lawful content, or from engaging in paid prioritization (referred to in the Order as "bright-line rules").[51] The April NPRM seeks to "reinstate the information service classification of broadband internet access service," revoking the FCC's ability to regulate these services as utilities (which are more heavily regulated), and to "seek comment on whether to keep, modify, or eliminate the bright-line rules set forth in the Title II Order."[52] The NPRM allows for the public to submit comments on the proposed changes before the FCC makes a decision; the public consultation period continued through August 30, after which the FCC is supposed to respond to the public's comments.[53]

44 David Shepardson, "Trump taps net neutrality opponent Ajit Pai to head FCC," *Reuters,* January 23, 2017, http://www.reuters.com/article/us-usa-trump-fcc-idUSKBN1572RK

45 Ashley Gold and John Hendel, "FCC back to full five members as net neutrality vote looms," *Politico*, August 3, 2017, http://www.politico.com/story/2017/08/03/fcc-nominees-confirmed-jessica-rosenworcel-brendan-carr-241298

46 Jim Puzzanghera, "FCC halts Internet privacy rule that imposes data security requirements on broadband providers," *Los Angeles Times*, March 1, 2017, http://www.latimes.com/business/la-fi-fcc-privacy-delay-20170301-story.html

47 Federal Communications Commission, "FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data," October 27, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A1.pdf

48 Brian Fung, "Republicans voted to roll back landmark FCC privacy rules. Here's what you need to know," *Washington Post,* March 28, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/?utm_term=.ac278467b9c0

49 Mike Snider, "How set to unplug broadband privacy rules," *USA Today*, March 28, 2017, https://www.usatoday.com/story/tech/news/2017/03/28/house-set-unplug-broadband-privacy-rules/99707178/

50 Federal Communications Commission, "Fact Sheet: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108," April 28, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

51 Federal Communications Commission, "Protecting and Promoting the Open Internet," March 12, 2015, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

52 Federal Communications Commission, "Fact Sheet: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108," April 28, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

53 Federal Communications Commission, "Fact Sheet: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108," April 28, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

# Limits on Content

*While the online environment in the United States continues to be vibrant and diverse, concerns over the proliferation of "fake news"—particularly on social media—heightened in the run-up to and aftermath of the November 2016 presidential election.*

## Blocking and Filtering

In general, the U.S. government does not block or filter online content. Some states require publicly funded schools to install filtering software on their computers to block obscene, illegal, or harmful content.[54] The Children's Internet Protection Act of 2000 (CIPA) requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing child pornography or visuals that are considered 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.[55] 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 decisions about filtering should be left to the discretion of individual libraries.[56]

## Content Removal

The government does not censor any particular political or social viewpoints, although legal rules do restrict certain types of content on the internet. Illegal online content, including child pornography and content that infringes on copyright, is subject to removal through a court order or similar legal process if it is hosted within the United States. Aside from these examples, government pressure on ISPs or content hosts to remove content is not a widespread issue. Social media companies and other content providers may remove content that violates their terms and conditions.

Content removal by private companies was brought into the spotlight in August 2016 when Facebook complied with a request from Baltimore police to temporarily disable Facebook and Instagram accounts operated by 23-year-old Korryn Gaines. Gaines was using her Facebook account to broadcast live as she used a shotgun to resist police attempting to serve her with an arrest warrant stemming from traffic violations. Later during the same encounter she was shot and killed, and her five-year-old son wounded.[57] Facebook subsequently restored her account, but restricted two videos it said violated its terms of service. Critics of Facebook's decision said the videos could have revealed more information about the circumstances of Gaines' death.[58] Smartphone videos of law enforcement shootings of African American citizens have drawn national media attention to cases that might otherwise be underreported and can support criminal charges against police

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

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

56 *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).

57 Baynard Woods, "Facebook deactivated Korryn Gaines' account during standoff, police say," *The Guardian,* August 3, 2016, https://www.theguardian.com/us-news/2016/aug/03/korryn-gaines-facebook-account-baltimore-police

58 Justin Fenton, "Korryn Gaines case: Video posting by suspects poses new challenges for police," *Baltimore Sun,* August 3, 2016, http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-facebook-police-deactivate-20160803-story.html

officers if they provide evidence of misconduct.[59] Individuals who have filmed shooting incidents have reported harassment by police (see "Prosecutions and Detentions for Online Activity" and "Intimidation and Violence").

One of the most significant protections for online free expression in the United States is Section 230 of the Communications Decency Act of 1934 (CDA 230), amended by the Telecommunications Act of 1996, which generally shields online sites and services from legal liability for the activities of their users, allowing user-generated content to flourish on a variety of platforms.[60] However, public concern over intellectual property violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of commercial trade secrets, gambling, financial crime, and terrorist content have presented a strong impetus for aggressive legislative and executive action, and some have threatened to undermine the broad protections of CDA 230.[61]

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. 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, 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.[62]

Intended to help protect against sex trafficking of children, the SAVE Act became law in May 2015.[63] The final text of the legislation was changed to make it illegal to knowingly advertise content related to sex trafficking, a higher requirement than an earlier draft that would have established liability for "knowledge of" or "active disregard for the likelihood of" hosting such content.[64] At the same time, the law still establishes federal criminal liability for third-party content, which could lead to companies choosing to over-censor rather than face criminal penalties, or to limit the practice of monitoring content altogether so as to avoid "knowledge" of illegal content.[65]

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).[66] Operating

59 David Uberti, "How smartphone video changes coverage of police abuse," *Columbia Journalism Review,* April 9, 2015, http://www.cjr.org/analysis/smartphone_video_changes_coverage.php

60 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.

61 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

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

63 The Justice for Victims of Trafficking Act of 2015, Pub. L 144-22, May 29, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/178

64 Sophia Cope and Adi Kamdar, "SAVE Act Passes in House, Comes One Step Closer to Unnecessarily Chilling Online Speech," Electronic Frontier Foundation, January 29, 2015, https://www.eff.org/deeplinks/2015/01/save-act-passes-house-coming-one-step-closer-chilling-online-speech

65 "Coalition Statement in Opposition to Federal Criminal Publishing Liability," Center for Democracy and Technology, January 29, 2015, https://cdt.org/insight/coalition-statement-in-opposition-federal-criminal-publishing-liability/

66 17 U.S.C.§ 512, https://www.law.cornell.edu/uscode/text/17/512

through a "notice-and-takedown" mechanism, internet companies are shielded from liability if they remove infringing content upon receipt of a DMCA notice. However, because companies have the incentive to err on the side of 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.[67] In some cases, the immediate removal of content through DMCA requests has been used to target political campaign advertisements, since they are unlikely to be challenged in court after the campaign ends and achieve the goal of making the content unavailable during the campaign season.[68]

Major internet companies, including Google, Twitter, Facebook, Microsoft, AT&T and Yahoo, publish information about removal requests from governments based on local laws. In its most recent report, Twitter reported receiving two court orders and 100 U.S. government or law enforcement requests to remove or withhold content between July and December of 2016, although it did not comply with any of these requests.[69] During the same period, Facebook reported that it did not receive any U.S. government requests to remove content,[70] while Yahoo reported receiving four U.S. government removal requests and complied with 50 percent of them.[71]

## Media, Diversity, and Content Manipulation

While the online environment in the United States continues to be vibrant and diverse, the prevalence of disinformation and partisan media has had a significant impact on the online media landscape. Concerns over the proliferation of "fake news"—particularly on social media—heightened in the run-up to and aftermath of the November 2016 presidential election. Internet users continue to exercise self-censorship due to concerns of government surveillance as well as online harassment by other internet users.

Manipulation of social media and its role in influencing the election was a prominent topic in the latter half of 2016. In May 2016, after Facebook received criticism for alleged anti-conservative bias in how its employees edit the "trending topics" feature of its platform,[72] the company reported that it was removing human editors from the process and relying solely on its algorithm to populate headlines, causing an immediate spike in fake news articles from all sides of the political spectrum.[73] In some cases, the source of these articles—which often feature blatantly false information and "click-bait" headlines—came from average internet users (rather than journalists) who were

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

68 Electronic Frontier Foundation, "Once Again, DMCA Abused to Target Political Ads," November 17, 2015, https://www.eff.org/deeplinks/2015/11/once-again-dmca-abused-target-political-ads

69 Twitter , "Removal Requests," *Transparency Report,* July-December, 2016, https://transparency.twitter.com/en/removal-requests.html

70 See download data: Facebook, "Government Requests Report: United States," July-December 2016, https://govtrequests.facebook.com/country/United%20States/2016-H2/

71 Yahoo, "Government Removal Requests," July-December 2016, https://transparency.yahoo.com/government-removal-requests

72 Michael Nunez, "Former Facebook Workers: We Routinely Suppressed Conservative News," *Gizmodo*, May 9, 2016, http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006

73 Abby Ohlheiser, "Three days after removing human editors, Facebook is already trending fake news," *Washington* Post, August 29, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/08/29/a-fake-headline-about-megyn-kelly-was-trending-on-facebook/. Annalee Newitz, "Facebook fires human editors, algorithm immediately posts fake news," Ars Technica, August 29, 2016, https://arstechnica.com/business/2016/08/facebook-fires-human-editors-algorithm-immediately-posts-fake-news/

capitalizing on the resulting ad revenue: a *Guardian* report in August 2016 identified more than 150 pro-Trump fake news sites promulgated by internet users in a small town in Macedonia, for example.[74]

Hyperpartisan media outlets and social media users continued to flourish online and affect the visibility of and attention paid to more balanced sources of news and information. In March 2016, several top executives and journalists of *Breitbart News*, a conservative political news website founded in 2007, resigned following an incident with a *Breitbart* journalist who was harassed at a Trump campaign rally, arguing that the company had failed to support the journalist and claiming that *Breitbart* had become "a shill for the Trump campaign."[75] The allegation of an alliance between *Breitbart* and the Trump campaign was bolstered when, on August 17, Trump named *Breitbart* chairman Steve Bannon as chief executive of his campaign.[76]

A study of the online political media ecosystem by researchers at MIT Media Law, Harvard Law School, and the Berkman-Klein Center for Internet and Society, found *Breitbart* at the center of a hyperpartisan right-wing media network.[77] By reviewing over 1.25 million stories published online between April 1, 2015 and November 8, 2016, the researchers found that many of the most-shared stories in this network centered around disinformation—"the purposeful construction of true or partly true bits of information into a message that is, at its core, misleading"—and that this pro-Trump online network successfully set the agenda for the conservative media sphere, exerting an outsized influence over more mainstream conservative news outlets as well as strongly influencing the broader media agenda, including media coverage of Hillary Clinton's campaign.[78] A study conducted by the Pew Research Center in December 2016 found that the majority of Americans—64 percent—felt that fabricated news stories caused "a great deal of confusion about the basic facts" of current events.[79]

Disinformation propagated by Russian internet trolls also played a role in the media ecosystem before and after the U.S. presidential election. Russian disinformation campaigns targeting U.S. communities and local news outlets are not new—for example, in June 2015, journalist Adrian Chen wrote a story for the *New York Times* about the Internet Research Agency, a "troll farm" based in Saint Petersburg, Russia, which Russian investigative journalists claim is funded by a local oligarch with close ties to President Vladimir Putin. Chen detailed examples of Russian trolls, posing as American Twitter users, launching coordinated disinformation campaigns attempting to trick observers into thinking that there had been an explosion at a chemical plant in Centerville,

74 Dan Tynan, "How Facebook powers money machines for obscure political 'news' sites," August 24, 2016, https://www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump

75 Michael M. Grynbaum, "Upheaval at Breitbart News as Workers Resign and Accusations Fly," *New York Times*, March 14, 2016, https://www.nytimes.com/2016/03/15/business/media/upheaval-at-breitbart-news-as-workers-resign-and-accusations-fly.html

76 Jonathan Martin, Jim Rutenberg, and Maggie Haberman, "Donald Trump Appoints Media Firebrand to Run Campaign," *New York Times*, August 17, 2016, https://www.nytimes.com/2016/08/18/us/politics/donald-trump-stephen-bannon-paul-manafort.html

77 Yochai Benkler, Robert Faris, Hal Roberts, and Ethan Zuckerman, "Study: Breitbart-led right-wing media ecosystem altered broader media agenda," *Columbia Journalism Review*, March 3, 2017, https://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php

78 Yochai Benkler, Robert Faris, Hal Roberts, and Ethan Zuckerman, "Study: Breitbart-led right-wing media ecosystem altered broader media agenda," *Columbia Journalism Review*, March 3, 2017, https://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php

79 Michael Barthel, Amy Mitchell, Jesse Holcomb, "Many Americans Believe Fake News is Sowing Confusion," Pew Research Center, December 15, 2016, http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/

Louisiana, or that an Ebola outbreak had occurred in Atlanta.[80] These troll networks continued to churn out disinformation surrounding the U.S. presidential election. In several instances, Donald Trump and members of his campaign staff propagated conspiracy theories or referenced fake events which, separately, were also reported by Russian state media outlets.[81] During his testimony before the Senate in March 2017, Clinton Watts, a senior fellow at the Foreign Policy Research Institute, argued that part of why Russian "active measures" were influential in the U.S. election was because the themes of these disinformation campaigns were "parroted" by the Trump campaign.[82] A representative from Facebook estimated that trolls associated with the Internet Research Agency shared 80,000 posts on its platform between June 2015 and August 2017. The posts—characterized by Facebook as "divisive social and political messages across the ideological spectrum"—ranged from support for Black Lives Matter, Bernie Sanders, and the National Rifle Association, to memes that were anti-Muslim or anti-immigrant.[83] The IRA spent around $100,000 to amplify the visibility of their posts, which reached some 126 million American users.[84] According to Twitter, over 36,000 Russia-linked automated accounts posted 1.4 million election-related tweets, receiving 288 million views from September 1 to November 15, 2016. The company noted these tweets represented less than one percent of all election-related tweets on the platform during that period.[85]

An increasingly partisan media environment also negatively impacted the ability of journalists from several online media outlets to cover the presidential campaigns and the Trump presidency. During the 2016 presidential race, Donald Trump's campaign refused to issue press credentials for several media outlets whose coverage they deemed unfavorable. Reporters from the online media outlets *Buzzfeed, Politico, Huffington Post*, and the *Daily Beast*, as well as from broadcast and traditional media like the *Washington Post*, Univision, and the *Des Moines Register*, were periodically prevented from attending Trump campaign press events and rallies.[86] These restrictions—and the threat of being banned or blacklisted for unfavorable coverage—risked inhibiting objective reporting on his candidacy.[87] On October 13, 2016, the board of the press freedom advocacy organization Committee to Protect Journalists issued a statement declaring that Trump's behavior as a presidential candidate signaled a threat to press freedom in the United States and could embolden authoritarian leaders abroad.[88]

80 Adrien Chen, "The Agency," *New York Times*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html

81 Linda Qui, "Trump campaign chair misquotes Russian media in bogus claim about NATO base terrorist attack," Politifact, August 16, 2016, http://www.politifact.com/truth-o-meter/statements/2016/aug/16/paul-manafort/trump-campaign-chair-misquotes-russian-media-makes/; Brian Naylor, "Trump Apparently Quotes Russian Propaganda to Slam Clinton on Benghazi," NPR, October 11, 2016, http://www.npr.org/2016/10/11/497520017/trump-apparently-quotes-russian-propaganda-to-slam-clinton-on-benghazi

82 Clint Watts, Testimony before Senate Select Intelligence Committee, March 30, 2017, https://www.c-span.org/video/standalone/?c4664397/clint-watts-3302017

83 April Glaser, "What Was Russia up To?" *Slate*, October 11, 2017, http://www.slate.com/articles/technology/future_tense/2017/10/what_we_know_about_russia_s_use_of_american_facebook_twitter_and_google.html

84 Committee on the Judiciary, "Hearing before the United States Senate Committee on the Judiciary Subcommittee on Crime and Terrorism: Testimony of Colin Stretch," October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf

85 Sean Edgett, "U.S. Senate Committee on the Judiciary: Opening Remarks," Twitter Blog, October 31, 2017, https://blog.twitter.com/official/en_us/topics/company/2017/opening_remarks.html

86 Tom Kludt and Brian Stelter, "'The Blacklist:' Here are the media outlets banned by Donald Trump," CNN, June 14, 2016, http://money.cnn.com/2016/06/14/media/donald-trump-media-blacklist/

87 Kyle Blaine, "How Donald Trump Bent Television To His Will," Buzzfeed, March 18, 2016, https://www.buzzfeed.com/kyleblaine/how-donald-trump-bent-television-to-his-will?utm_term=.ioJba25Rz#.rmPn4K85k

88 "CPJ chairman says Trump is threat to press freedom," Committee to Protect Journalists, October 13, 2016, https://cpj.org/2016/10/cpj-chairman-says-trump-is-threat-to-press-freedom.php.

Trump continued to place restrictions on the press during the first few months of his presidency. On February 24, the White House blocked journalists from several media outlets, including CNN, the *New York Times, Politico,* and *Buzzfeed*, from attending a White House press briefing.[89] In May 2017, leaks about conversations between President Trump and James Comey, then-director of the FBI, revealed that Trump had encouraged Comey to jail journalists who published classified information, which journalists, editors, and press freedom groups spoke out against as an intimidation tactic.[90]

Reports of self-censorship among journalists, lawyers, and everyday internet users persist. Online harassment is one of the driving forces behind self-censorship: a 2016 study by researchers at the Data & Society Research Institute and the Center for Innovative Public Health Research found that 27 percent of Americans self-censor due to fear of online harassment.[91] According to the research findings, young women are more likely to report self-censoring than older women or men, and "Black, LGB individuals, and people living in higher income households are also more likely than White, non-LGB, and lower income individuals, respectively, to self-censor."[92]

Journalists report that their ability to investigate and publish freely has been chilled in recent years due to government pressure and threats to the security of their digital communications. 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. 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.[93] A grand jury investigation into WikiLeaks has been ongoing since 2011.[94] On March 17, 2017, Reuters reported that federal prosecutors were expanding the investigation to include the trove of CIA documents posted on March 7.[95]

Ordinary American citizens have also changed their behavior in response to extensive government surveillance. A study published in *Journalism & Mass Communication Quarterly* in February 2016 found that priming participants with subtle reminders about mass surveillance had a chilling effect

89 Ayesha Rascoe, "White House bars some news organizations from briefing," Reuters, February 24, 2017, http://www.reuters.com/article/us-usa-trump-media-idUSKBN1632JG

90 Michael M. Grynbaum, Sydney Ember, and Charlie Savage, "Trump's Urging That Comey Jail Reporters Denounced as an 'Act of Intimidation,'" *New York Times*, May 17, 2017, https://www.nytimes.com/2017/05/17/business/media/trumps-urging-that-comey-jail-reporters-denounced-as-an-act-of-intimidation.html

91 Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, "Online Harassment, Digital Abuse, and Cyberstalking in America," Data & Society and the Center for Innovative Public Health Research, November 21, 2016, https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

92 Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, "Online Harassment, Digital Abuse, and Cyberstalking in America," Data & Society and the Center for Innovative Public Health Research, November 21, 2016, p. 53, https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

93 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

94 Glenn Greenwald, "FBI serves Grand Jury subpoena likely relating to WikiLeaks," *Salon*, April 27, 2011, http://www.salon.com/2011/04/27/wikileaks_26/

95 Mark Hosenball, "U.S. prosecutors probing leak of CIA material to WikiLeaks: sources," *Reuters*, March 17, 2017, http://www.reuters.com/article/us-cia-wikileaks-idUSKBN16O2S2?il=0

on individuals' willingness to publicly express minority opinions online.[96]

Diversity of content online is ensured in part through the protection 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. With the FCC's Republican leadership signaling its intent to roll back net neutrality protections, it is unclear whether there will be strong enough accountability mechanisms to ensure that ISPs treat all lawful internet traffic equally, although as of May 2017 the net neutrality protections were still in effect (see "Regulatory Bodies"). The FCC approved an Open Internet Order in 2015 that prohibits blocking and unreasonable discrimination on both fixed and wireless networks, reflecting the growing importance of mobile broadband in the United States. On June 14, 2016, the federal appeals court in Washington, DC upheld the FCC's authority to issue the Open Internet Order, further solidifying the principle of net neutrality.[97]

In February 2017, the FCC announced it was cancelling its investigation into mobile providers' zero-rating practices,[98] which allow unlimited streaming of video content from some services but not from others.[99] In March 2016, more than 50 advocacy groups had signed a letter to the FCC Chairman at the time, Tom Wheeler, arguing that zero-rating practices violate net neutrality and the spirit of the Open Internet Order, though it does not explicitly prohibit them.[100]

## Digital Activism

Political activity in the United States has increasingly moved online in recent years.[101] The Women's March on Washington, which took place on the Saturday immediately following President Trump's inauguration, was largely coordinated using social media platforms: details were spread via Facebook, Twitter, and Instagram, encouraging anyone who supported the march's platform to join or start their own local march.[102] In total, more than 4.2 million people participated in 600 cities around the country, in what some researchers estimate was the largest protest in American history.[103]

The Black Lives Matter movement—which started in 2013 with the hashtag #blacklivesmatter—has

96 Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly,* 2016, http://m.jmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf; Karen Turner, "Mass surveillance silences minority opinions, according to study," *Washington Post*, March 28, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/

97 Alina Selyukh, "U.S. Appeals Court Upholds Net Neutrality Rules in Full," NPR, June 14, 2016, http://www.npr.org/sections/thetwo-way/2016/06/14/471286113/u-s-appeals-court-holds-up-net-neutrality-rules-in-full

98 Aaron Pressman, "Trump's FCC Moving to Kill Probes of Zero Rating by AT&T and Verizon," *Fortune*, February 3, 2017, http://fortune.com/2017/02/03/trump-fcc-zero-rating-att-verizon/

99 Cecilia Kang, "F.C.C. Asks Comcast, AT&T and T-Mobile About 'Zero-Rating' Services," *The New York Times*, December 17, 2015, http://bits.blogs.nytimes.com/2015/12/17/f-c-c-asks-comcast-att-and-t-mobile-about-zero-rating-services/

100 Zero rating letter to FCC, March 28, 2016, https://www.eff.org/files/2016/04/07/finalzeroratingsign-onletter.fa929bef59a5423089a496b4f909fb97.pdf

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

102 Paul Farhi, "How mainstream media missed the march that social media turned into a phenomenon," *Washington Post*, January 22, 2017.

103 Sarah Frostenson, "The Women's Marches may have been the largest demonstration in US history," *Vox*, January 31, 2017, https://www.vox.com/2017/1/22/14350808/womens-marches-largest-demonstration-us-history-map

become a prominent example of a "decentralized but coordinated"[104] social justice movement that has strategically used social media to organize protests against police violence and shift national conversations about race. Information released by Twitter revealed that the #blacklivesmatter hashtag had been used over 12 million times since it started, making it the third most used hashtag on the platform.[105]

An unprecedented number of Americans used online tools to mobilize in support network neutrality. 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.[106] 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 media.[107] 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.[108] 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.[109]

## Violations of User Rights

*The United States has a robust legal framework that supports freedom of expression both online and offline, and the government does not typically prosecute individuals for online speech or activities unless a crime is committed. The broader picture of user rights in America, however, has become increasingly complex. Government surveillance is a major concern, especially following revelations about NSA practices, although several of these programs were reformed following the passage of the USA FREEDOM Act in June 2015. In addition, the privacy of NGOs, companies, government agencies, and individual users is threatened by a growing number of cyberattacks initiated by both domestic and international actors. Threatening or antisemitic social media messages against journalists also increased during the year.*

### Legal Environment

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

104 Bijan Stephen, "How Social Media Helps Black Lives Matter Fight the Power," *Wired*, November 2015, https://www.wired.com/2015/10/how-black-lives-matter-uses-social-media-to-fight-the-power/

105 Tanya Sichynsky, "These 10 Twitter hashtags changed the way we talk about social issues," *Washington Post*, March 21, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/03/21/these-are-the-10-most-influential-hashtags-in-honor-of-twitters-birthday/?utm_term=.64b45645b2d3

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

107 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

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

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

constitutional protection.[110] Lower courts have consistently struck down attempts to regulate online content.

Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has fueled growing criticism of the 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.[111] In one prominent case from 2011, programmer and internet activist Aaron Swartz secretly used Massachusetts Institute of Technology servers to download millions of files from JSTOR, a service providing academic articles. Prosecutors sought harsh penalties for Swartz under CFAA, which could have resulted in up to 35 years imprisonment.[112] Swartz committed suicide in 2013 before he was tried. After his death, a bipartisan group of lawmakers introduced "Aaron's Law," a piece of 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.[113] The bill was reintroduced in 2015, but did not garner enough support to move forward.[114]

Companies are shielded from liability for the activities of their users by Section 230 of the Communications Decency Act (see "Content Removal"). 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.[115] A number of U.S. laws also protect speech from harmful corporate actions, 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 (see "Surveillance, Privacy, and Anonymity").

There are no legal restrictions on user anonymity on the internet, and constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[116] The legal framework for government surveillance, however, has been open to abuse. In June 2015, President Obama signed the USA FREEDOM Act into law, introducing some restrictions on the way the NSA can access information about American citizens from their phone records. Other laws used to authorize surveillance have yet to be reformed (see "Surveillance, Privacy, and Anonymity").

On April 3, 2017, President Trump signed S.J. Resolution 34, which nullified the FCC's broadband privacy guidelines (see "Regulatory Bodies").[117] The joint resolution rolled back regulations introduced in October 2016 that would have given consumers more control over how their personal information is collected and used by broadband internet service providers. On the other hand,

110 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

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

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

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

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

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

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

117 S,J. Resolution 34 – 115th Congress (2017-2018); Public Law no. 115-22, April 3, 2017, https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34

several states, including California, Minnesota, and Illinois, were considering legislation to protect internet users' privacy rights.[118] As of September 2017, the Illinois "right to know" bills (SB 1502 and HB 2774) were still being considered by the state legislature. The Minnesota bill had passed the state senate with widespread support from Republicans and Democrats but was later taken out of a larger spending bill during private negotiations.[119] On September 15, the California state legislature failed to pass AB 375, a broadband privacy bill aimed at addressing the rollback of the FCC guidelines for operators within the state.[120]

## Prosecutions and Detentions for Online Activities

Prosecutions or detentions for online activities, particularly for online speech, are relatively infrequent given broad protections under the First Amendment. However, there have been prosecutions related to threats posted on social media, arrests related to filming police interactions, and problematic prosecutions under the Computer Fraud and Abuse Act. In addition, Customers and Border Patrol agents at international airports are increasingly forcing travellers, including American citizens, to turn over their cell phone passcodes or risk detention.

Americans can be detained if they refuse to hand over their cell phone or reveal their cell phone passcode to border agents. Although they are not legally required to unlock their phones, the threat of detention or confiscation of their electronic devices can pressure individuals to comply. There has been a significant increase in warrantless searches of travellers' cell phones by border agents when travellers attempt to enter the United States, tripling from 857 searches in October 2015 to 2,560 searches in October 2016.[121] In one case, an American NASA engineer who was flying back from South America was detained and told to hand over the passcode for his phone, even though it was the property of the NASA lab where he worked.[122] On April 4, 2017, several senators introduced legislation that would require border patrol agents to obtain a warrant before searching the contents of a cell phone, and would prohibit agents from detaining people for more than four hours while trying to get them to unlock their phones.[123] The bill had not yet been voted on as of mid-2017.

Police have periodically detained individuals who uploaded images or broadcast live video of police activity with their phones, posing a threat to First Amendment protections.[124] Most of the arrests have been made on unrelated charges, such as obstruction or resisting arrest, since openly filming police activity is a protected right. In July 2016, police in Louisiana detained store owner Abdullah

118 Jon Brodkin, "ISP privacy rules could be resurrected by states, starting in Minnesota," *Ars Technica*, March 31, 2017, https://arstechnica.com/tech-policy/2017/03/isp-privacy-rules-could-be-resurrected-by-states-starting-in-minnesota/; See also: Conor Dougherty, "Push for Internet Privacy Rules Moves to Statehouses," *New York Times*, March 26, 2017, https://www.nytimes.com/2017/03/26/technology/internet-privacy-state-legislation-illinois.html?_r=0

119 Erin Golden, "Internet privacy measure removed as lawmakers debate budget," *Star Tribune*, May 2, 2017, http://www.startribune.com/internet-privacy-measure-removed-as-lawmakers-debate-budget/421030613/

120 "California Planned on Strengthening Internet Privacy. It Didn't," *Fortune,* September 18, 2017, http://fortune.com/2017/09/18/california-internet-privacy/

121 Cynthia McFadden, E.D. Cauchi, William M. Arkin, and Kevin Monahan, "American Citizens: U.S. Border Agents Can Search Your Cellphone," NBC News, March 13, 2017, http://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746

122 Loren Grush, "A US-born NASA scientist was detained at the border until he unlocked his phone," *The Verge*, February 12, 2017, https://www.theverge.com/2017/2/12/14583124/nasa-sidd-bikkannavar-detained-cbp-phone-search-trump-travel-ban

123 Cora Currier, "Lawmakers Move to Stop Warrantless Cellphone Searchers at the U.S. Border," *The Intercept*, April 4, 2017, https://theintercept.com/2017/04/04/lawmakers-move-to-stop-warrantless-cell-phone-searches-at-the-u-s-border/

124 Frank Eltman, "Citizens filming police often find themselves arrested," *Albuquerque Journal*, August 30, 2015, http://www.abqjournal.com/636460/citizens-filming-police-often-find-themselves-arrested.html

Muflahi for six hours and confiscated his cellphone after he filmed the fatal shooting of Alton Sterling by police.[125] Chris LeDay, a Georgia-based musician who shared another video of the same incident on Facebook, was arrested soon after for unpaid traffic fines.[126]

Several journalists were arrested or detained while covering protests on the day of President Trump's inauguration in January 2017. Evan Engel, an independent journalist who was a senior producer for Vocativ at the time, was arrested along with several hundred protesters and detained for 27 hours before release. He was charged with rioting, though the charges were later dropped.[127] A producer for the web series "Story of America" was also arrested, detained for 36 hours, and charged with a felony, though his charges were also dropped several days later.[128]

Amid heightened tensions following the shooting of five police officers in Dallas in July 2016, there was an increase in the number of arrests of civilians who posted threatening language on social media. The following week, four people were arrested in Detroit for posting threats to police on Facebook and Twitter; three of the cases were dropped due to lack of evidence needed to support criminal charges.[129] In October 2016, felony terrorist charges were brought against Detroit resident Nheru Gowan Littleton for posting messages on Facebook praising the shootings of the cops in Dallas and allegedly posting comments like "Kill all white cops!"[130] His trial began in March 2017; as of mid-2017, his trial had not yet reached a verdict.

Previously, the government used the Computer Fraud and Abuse Act to prosecute Matthew Keys, a former Tribune Company journalist and social media editor who had given log-in credentials to the hacking group Anonymous. Keys was convicted in October 2015 and sentenced to two years' imprisonment on April 13, 2016.[131] Some critics of CFAA argued that Keys' sentencing was overly harsh, and that many of his crimes could be charged as misdemeanors.[132] Many states also have their own laws related to computer hacking or unauthorized access. Several smaller cases in the past few years highlighted the shortcomings and lack of proportionality of these laws.[133]

125 Democracy Now! "Meet Abdullah Muflahi: He Filmed Alton Sterling Shooting and Was Then Detained by Baton Rouge Police," July 13, 2016, https://www.democracynow.org/2016/7/13/meet_abdullah_muflahi_he_filmed_alton

126 Rachel Ravesz, "Alton Sterling shooting: Man who posted video of killing arrested," *The Independent*, July 15, 2016, http://www.independent.co.uk/news/world/americas/alton-sterling-shooting-man-who-posted-video-of-killing-arrested-and-allegedly-harassed-by-police-a7139241.html

127 Press Freedom Tracker, "Vocativ journalist charged with rioting in Washington," January 20, 2017, https://pressfreedomtracker.us/all-incidents/vocativ-journalist-charged-with-rioting-in-washington/

128 Press Freedom Tracker, "Producer Jack Keller arrested at Trump inauguration protest," January 20, 2017, https://pressfreedomtracker.us/all-incidents/producer-jack-keller-arrested-trump-inauguration-protest/

129 "No charges for 3 making threats on Detroit cops," *The Detroit News,* August 31, 2016, http://www.detroitnews.com/story/news/local/detroit-city/2016/08/30/alleged-threat-detroit-cop-leads-arrest/89573042/

130 "Alleged Facebook threats against police lead to terrorist charges for Detroit man," *The Guardian,* October 5, 2016, https://www.theguardian.com/us-news/2016/oct/05/facebook-threats-white-police-officers-terrorist-charges

131 Christopher Mele, "Matthew Keys Gets 2 Years in Prison in Los Angeles Times Hacking Case," *New York Times*, April 13, 2016, http://www.nytimes.com/2016/04/14/business/media/matthew-keys-gets-2-years-in-prison-in-los-angeles-times-hacking-case.html

132 Kim Zetter, "Matthew Keys Sentenced to Two Years for Aiding Anonymous," *Wired*, April 13, 2016, https://www.wired.com/2016/04/journalist-matthew-keys-sentenced-two-years-aiding-anonymous/

133 Joe Johnson, "Georgia Tech student who hacked into UGA computer network gets pretrial diversion," *Athens Banner-Herald*, February 26, 2015, http://bit.ly/1FSEllk; See also: Josh Solomon, "Middle school student charged with cybercrime in Holiday," *Tampa Bay Times*, April 9, 2015, http://bit.ly/1ybpTBg

## Surveillance, Privacy, and Anonymity

The passage of the USA FREEDOM Act in June 2015 marked the most significant legislative reform to U.S. surveillance practices in recent decades. Despite this reform, however, a number of problematic provisions remained in effect, such as programs authorized by Section 702 that enabled the incidental collection of Americans' communications and metadata. In April 2017, the NSA announced that it would amend a practice known as "upstream" collection, authorized under Section 702, to limit the incidental collection of American's communications.

Under a set of complex statutes, U.S. law enforcement and intelligence agencies can monitor communications content and communications records, or metadata, under varying degrees of oversight as part of criminal or national security investigations. The government may request that companies store such data for up to 180 days under the Stored Communications Act, but how they otherwise collect and store communications content and records varies by company.[134]

Law enforcement access to metadata generally requires a subpoena issued by a prosecutor or investigator without judicial approval;[135] a warrant is only required in California under the California Electronic Communications Privacy Act, which went into effect on January 1, 2016.[136] 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.[137] 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 subpoena.[138] In April 2016, the House of Representatives passed the Email Privacy Act, which would require the government to obtain a probable cause warrant before accessing email or other private communications stored with cloud service providers.[139] The bill was reintroduced in January 2017, passed the House, and was awaiting review in the Senate.[140]

The USA PATRIOT Act, passed following the terrorist attacks of September 11, 2001, expanded government surveillance and investigative powers in terrorism and criminal investigations.[141] On June 2, 2015, President Obama signed the USA FREEDOM Act into law, extending expiring provisions

134 Electronic Frontier Foundation, "Mandatory Data Retention: United States," https://www.eff.org/issues/mandatory-data-retention/us

135 Electronic Frontier Foundation, "Mandatory Data Retention: United States;" Center for Constitutional Rights, "Surveillance After the USA Freedom Act: How Much Has Changed?," *Huffington Post,* December 17, 2015, http://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html

136 American Civil Liberties Union, "California Electronic Communications Privacy Act (CalECPA) - SB 178," https://www.aclunc.org/our-work/legislation/calecpa

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

138 Ibid.

139 Sophia Cope, "House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform," Electronic Frontier Foundation, April 27, 2016, https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform

140 H.R. 387 Email Privacy Act, https://www.congress.gov/bill/115th-congress/house-bill/387/text

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

of the PATRIOT Act, including broad authority to conduct roving wiretaps of "John Doe" targets and "lone wolf" surveillance.[142] On the other hand, the law significantly reformed the bulk collection of phone records under Section 215, a program detailed in documents leaked by former NSA contractor Edward Snowden in 2013,[143] and ruled illegal by the Second Circuit of Appeals in May 2015.[144]

The USA FREEDOM Act replaced the bulk collection program with a system that allows the NSA to access records held by phone companies with an order from the Foreign Intelligence Surveillance Court (FISA court).[145] Requests for that access require the use of a "specific selection term" (SST) representing an "individual, account, or personal device,"[146] which is intended to prohibit broad requests for records based on zip code or other indicators, and can only be extended or renewed in certain circumstances.[147] The SST provision also applies when intelligence agents use FISA pen registers and trap and trace devices, instruments that will capture a phone's outgoing or incoming records, and to national security letters, secret subpoenas to request call records issued by the FBI.[148]

The USA FREEDOM Act also required that the FISA court appoint an *amicus curiae*, an individual (or several) qualified to provide legal arguments that "advance the protection of individual privacy and civil liberties."[149] Six individuals have since been designated to serve as an amicus curiae.[150]

Despite these significant improvements, other surveillance programs revealed by the NSA leaks were authorized under laws which, though partially reformed since they were exposed in 2013, still contain scope for surveillance that lacks oversight, specificity, and transparency:

- *Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008*: Section 702 was used to authorize PRISM and "Upstream" collection, the controversial programs under which the NSA reportedly collects users' communications data—including the content—directly from U.S. tech companies and through the physical infrastructure of undersea cables.[151] Section 702 only authorizes the collection of information about foreign citizens, yet the content of Americans' communications swept up in this process is also collected and stored in a searchable database.[152] The USA FREEDOM Act made no changes

142 "USA Freedom Act: What's in, what's out," *Washington Post,* June 2, 2015, https://www.washingtonpost.com/graphics/politics/usa-freedom-act/

143 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

144 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

145 Aarti Shahani, "Phone Carriers Are Tight-Lipped On How They Will Comply With New Surveillance Law," NPR, June 4, 2015, http://www.npr.org/sections/alltechconsidered/2015/06/04/411870819/phone-carriers-are-tight-lipped-over-law-that-overhauls-nsa-surveillance

146 Rainey Reitman, "The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done," Electronic Frontier Foundation, April 30, 2015, https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done

147 "USA Freedom Act of 2015," Council on Foreign Relations, June 2, 2015, http://www.cfr.org/intelligence/usa-freedom-act-2015/p36594

148 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. 114-23, June 1, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2048/text

149 USA FREEDOM Act of 2015, Sec. 401.

150 United States Foreign Intelligence Surveillance Court, "Amici Curiae," http://www.fisc.uscourts.gov/amici-curiae

151 Brett Max Kaufman, "A Guide to What We Know About the NSA's Dragnet Searches of Your Communications," ACLU, August 9, 2013, https://www.aclu.org/blog/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications

152 Dia Kayyali, "The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why." Electronic Frontier Foundation, May 7, 2014, https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why

to this practice or to the NSA's access to the communications content collected. It limits the use of information about U.S. citizens in court or in other government proceedings if the NSA did not follow existing procedures to minimize the likelihood of collecting that information. The FISA court will determine whether or not those procedures were followed.[153]

- In October 2016, during the FISA court's annual review and reauthorization of surveillance conducted under Section 702, the government notified the FISA court judge that it had reported widespread violations of protocols intended to limit access to Americans' communications by NSA analysts (these details were revealed when the information was declassified in May 2017).[154] "Upstream" collection, which captures any communications that mention a foreign target, not just communications to and from a foreign target, is more likely than other programs to incidentally collect communications sent between U.S. citizens, which is outside the scope of lawful surveillance.[155] The report showed analysts had failed to take steps to ensure that they are not searching the upstream database when conducting queries.

- In response, the court delayed reauthorizing the program, and in April 2017 the NSA director recommended that the agency halt its collection of Americans' communications that merely mentioned a surveillance target (referred to as "about collection"), and instead only collect communications to and from the target.[156] Privacy advocates welcomed the decision by the NSA to halt this type of collection, and emphasized that the government's findings underscore the need for legislative reform of Section 702, which is set to expire in December 2017.[157] Advocates have argued that, in addition to codifying this ban on "about collection," reforms to Section 702 should include, among other things, limiting the degree to which collected communications are used for domestic law enforcement,[158] and closing the "backdoor search loop" that currently permits intelligence agents to run warrantless searches on data that has been collected under Section 702.[159]

- *Executive Order 12333*: Originally issued in 1981, Executive Order 12333 outlines how and when the NSA or other agencies may conduct surveillance on U.S. citizens and other individuals within the United States,[160] authorizing the collection of U.S. citizens' metadata

153 See USA FREEDOM Act of 2015, Sec. 301, and 50 U.S.C. 1881a(i)(3), available at: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap36-subchapVI-sec1881a.pdf

154 Charlie Savage, "How Trump's NSA Came to End a Disputed Type of Surveillance," *New York Times*, May 11, 2017, https://www.nytimes.com/2017/05/11/us/politics/nsa-surveillance-trump.html

155 Charlie Savage, "How Trump's NSA Came to End a Disputed Type of Surveillance," *New York Times*, May 11, 2017, https://www.nytimes.com/2017/05/11/us/politics/nsa-surveillance-trump.html

156 Charlie Savage, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets," *New York Times*, April 28, 2017, https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html

157 "OTI Applauds End to NSA 'About Collection,' Urges Statutory Reform Section 702," Open Technology Institute, April 28, 2017, https://www.newamerica.org/oti/press-releases/oti-applauds-end-nsa-about-collection-urges-statutory-reform-section-702/; "NSA Halts Part of Invasive Surveillance Program, Need for Section 702 Reform Highlighted," Center for Democracy & Technology, April 28, 2017, https://cdt.org/press/nsa-halts-part-of-invasive-surveillance-program-need-for-section-702-reform-highlighted/

158 Jake Laperruque, "How Congress Should Evaluate Section 702's Security Value When Debating its Reauthorization," June 16, 2017, https://www.lawfareblog.com/how-congress-should-evaluate-section-702s-security-value-when-debating-its-reauthorization

159 Robyn Greene, "OTI Reform Priorities for Section 702 of the FISA Amendments Act," Open Technology Institute, May 2, 2017, https://www.newamerica.org/oti/blog/otis-reform-priorities-section-702-fisa-amendments-act/

160 Executive Order 12333—United States Intelligence Activities. Federal Register, National Archives. http://www.archives.gov/federal-register/codification/executive-order/12333.html

and the content of communications if that data is collected "incidentally."[161] The extent of current NSA practices authorized under EO12333 is unclear, but documents from the NSA leaks suggest that EO12333 was used to authorize the so-called "MYSTIC" program, which was reportedly used to capture all of the incoming and outgoing phone calls of one or more target countries on a rolling basis. *The Intercept* identified the Bahamas, Mexico, Kenya, and the Philippines as targets in 2014.[162] In December 2014, Congress passed a law that included a requirement that the NSA develop "procedures for the retention of incidentally acquired communications" collected pursuant to EO12333, and that such communications may not be retained for more than five years except when subject to certain broad exceptions.[163] In January 2015, the president updated a 2014 policy directive that put in place important new restrictions relevant to EO12333 on the use of information collected in bulk for foreign intelligence purposes.[164] Civil society groups continue to campaign for its complete reform.[165]

The USA FREEDOM Act also changed the way private companies publicly report on government requests they receive for user information. The U.S. Department of Justice (DOJ) limits the disclosure of information about national security letters, including in the transparency reports voluntarily published by some internet companies and service providers.[166] In 2014, the DOJ 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.[167] Twitter, not a party to the settlement, filed suit against the DOJ in October 2014 on grounds that the rules amount to an unconstitutional prior restraint that violates the company's First Amendment rights.[168] In May 2016, a judge partially dismissed Twitter's case but gave them the opportunity to refile.[169] The USA FREEDOM Act allows companies the option of more granular reporting, though reports containing more detail are still subject to time delays and their frequency is limited.[170]

User data is otherwise protected under Section 5 of the Federal Trade Commission Act (FTCA), which 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,

161 "Executive Order 12333," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/12333/

162 Barton Gellman and Ashkan Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *Washington Post*, March 18, 2014, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html ; Ryan Devereaux, Glenn Greenwald, Laura Poitras, "Data Pirates of the Caribbean," *The Intercept*, May 19, 2014, https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

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

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

165 Human Rights Watch, "Strengthen the USA Freedom Act," May 19, 2015, https://www.hrw.org/news/2015/05/19/strengthen-usa-freedom-act

166 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

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

168 Ben Lee, "Taking the fight for #transparency to court," *Twitter Blog*, October 7, 2014, http://bit.ly/Zc3Mtm ; Alexei Oreskovic, "Twitter Sues U.S. Justice Department for Right to Reveal Surveillance Requests," *Reuters,* October 7, 2014, http://reut.rs/1yLKbRe

169 "Twitter lawsuit partly dismissed over U.S. information requests," Reuters, May 2, 2016, http://www.reuters.com/article/us-twitter-government-ruling-idUSKCN0XT1RK

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

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 Telecommunications Act prohibits telecommunications carriers from 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 also applied to ISPs' records about broadband customers.[171]

While there are no legal restrictions on anonymous communication online, some social media platforms require users to register using their real names through Terms of Service or other contracts.[172] Online anonymity has been challenged in cases involving hate speech, defamation, or libel. In one recent example, a Virginia court tried to compel the crowdsourced review platform Yelp to reveal the identities of anonymous users, before the Supreme Court of Virginia ruled that they did not have the authority.[173]

Recent cases have also raised the question of the degree to which the courts can force technology companies to comply with court orders, particularly those that would require the companies to alter their products. Following a terrorist attack in San Bernardino in December 2015, the U.S. government sought to compel Apple to unlock a passcode-protected iPhone belonging to one of the perpetrators. Because some iPhones are programmed to permanently block access to all of the phone's encrypted data once an incorrect passcode is entered too many times, the government issued a court order that would compel Apple to create new software enabling the FBI to access the phone.[174] Security experts argued that requiring companies to create "backdoors" for law enforcement to access encrypted data would undermine security and public trust.[175]

Conversely, there have been efforts to codify rules that would bar the government from requiring surveillance backdoors. In 2014, the U.S. House of Representatives approved an amendment to a bill governing appropriations which would ban spending on government-mandated backdoors with overwhelming bipartisan support, although later negotiations prevented it from being adopted into the final bill.[176] The House approved two similar amendments in 2015.[177] 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

171 Alex Bradshaw, Stan Adams, "FCC Should Act to Protect Broadband Customers' Data," CDT, January 20, 2016, https://cdt.org/blog/fcc-should-act-to-protect-broadband-customers-data/

172 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

173 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

174 Julia Angwin, "What's Really At Stake in the Apple Encryption Debate," ProPublica, February 24, 2016, https://www.propublica.org/article/whats-really-at-stake-in-the-apple-encryption-debate

175 Press Release, "Open Technology Institute Opposes Government Attempt to Mandate Backdoor into Apple iPhone," Open Technology Institute, February 17, 2016, https://www.newamerica.org/oti/press-releases/open-technology-institute-opposes-government-attempt-to-mandate-backdoor-into-apple-iphone/

176 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

177 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

backdoors to facilitate access.[178] As of mid-2017, no further action had been taken.

Despite vigorous debate, there have been no legislative changes 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.[179] 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.[180] Calls to update CALEA to cover online applications and communications have not been successful. In 2013, 20 technical experts published a paper explaining why such a proposal (known as "CALEA II") would create significant internet security risks.[181]

Other legal implications of law enforcement access to devices have been debated in the courts. In March 2016, a Maryland state appellate court issued a ruling stating that law enforcement must obtain a warrant before using "covert cell phone tracking devices" known by the product name Stingray.[182] Stingray devices act like cell phone towers, causing nearby cell phones to send it identifying information and thus allowing law enforcement to track targeted phones or determine the phone numbers of people in a nearby area. In its decision, the court rejected the argument that individuals are effectively "volunteering" their private information when they choose to turn on their phones, since doing so allows third parties (the phone company's cell towers) to send and receive signals from the phone.[183] This was the first court decision addressing whether a warrant is required in the use of Stingray devices[184]

On May 18, 2017, *The Detroit News* obtained court documents showing that police had used Stingray devices to find and arrest an undocumented immigrant.[185] Privacy advocates argue that because Stingray devices collect information from cell phones in the area surrounding the target, and thus constitute mass surveillance, their use by law enforcement should be limited to serious cases involving violent crimes, not immigration violations.[186]

In addition to surveilling private communications, law enforcement agencies have also monitored websites and social media platforms for suspected criminal activity. In October 2016, the ACLU reported that police were conducting social media surveillance using a tool called Geofeedia, which

178 Secure Data Act of 2014, S.2981, 113th Cong. (2014), http://1.usa.gov/1Lc1Eme

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

180 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

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

182 Spencer S. Hsu, "A Maryland court is the first to require a warrant for covert cellphone tracking," *Washington Post,* March 31, 2016, https://www.washingtonpost.com/world/national-security/a-maryland-court-is-the-first-to-require-a-warrant-for-covert-cellphone-tracking/2016/03/31/472d9b0a-f74d-11e5-8b23-538270a1ca31_story.html

183 Joshua Kopstein, "Maryland Attorney General: If You Don't Want To Be Tracked, Turn Off Your Phone," *Motherboard,* February 4, 2016, https://motherboard.vice.com/read/maryland-attorney-general-if-you-dont-want-to-be-tracked-turn-off-your-phone

184 Alex Emmons, "Maryland Appellate Court Rebukes Police for Concealing Use of Stingrays," *The Intercept,* March 31, 2016, https://theintercept.com/2016/03/31/maryland-appellate-court-rebukes-police-for-concealing-use-of-stingrays/

185 Robert Snell, "Feds use anti-terror tool to hunt the undocumented,"

186 Adam Schwartz, "No Hunting Undocumented Immigrants with Stingrays," Electronic Frontier Foundation, May 19, 2017, https://www.eff.org/deeplinks/2017/05/no-hunting-undocumented-immigrants-stingrays

allows users to aggregate social media content by location (such as a protest site); the company specifically marketed its service to law enforcement agencies.[187] Following the ACLU's report, Facebook, Twitter, and Instagram shut off Geofeedia's access to their data.[188]

On March 8, 2017, the ACLU announced that it was filing a motion to quash a warrant that a local law enforcement office in Washington state had obtained to search the private and public communications and location data related to users of a local Facebook group against the construction of the Dakota Access Pipeline.[189] The ACLU argued that the warrant was overbroad and could have a chilling effect on political speech and civic participation. [190] On March 13, the county withdrew the warrant request.[191] Also in March, U.S. Customs and Border Protection agents asked Twitter to reveal the owner of an account that objected to Trump's immigration policy, and backed off only after the company filed a lawsuit against the request.[192]

## Intimidation and Violence

Journalists face increased levels of harassment and threats online. According to a report by the Anti-Defamation League, antisemitic posts on Twitter increased significantly from January to July of 2016, correlating with "intensifying" coverage of the presidential political campaigns. The report found that at least 800 journalists had received anti-Semitic tweets between August 2015 and July 2016.[193] Journalists also face threats for writing about political topics, particularly in the highly charged and often vitriolic environment of online public discourse. Several journalists have reported being doxxed—having their home addresses, phone numbers, and other personal details posted online—and have received violent threats directed at themselves or their family members, causing them to think twice before writing about potentially controversial topics.[194]

Bloggers and other ICT users generally are not subject to extralegal intimidation or violence from state actors. However, police have used intimidation and threats to discourage bystanders from filming or uploading footage, particularly surrounding protests related to police violence against African Americans. Citizens have a legal right to film police interactions openly if they are not

187 Jonah Engel Bromwich, Daniel Victor, and Mike Isaac, "Police Use Surveillance Tool to Scan Social Media, A.C.L.U Says," *New York Times*, October 11, 2016, https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html

188 Jonah Engel Bromwich, Daniel Victor, and Mike Isaac, "Police Use Surveillance Tool to Scan Social Media, A.C.L.U Says," *New York Times*, October 11, 2016, https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html

189 "Warrant served on Facebook is overbroad and violates first and fourth amendments, ACLU argues in court filing," American Civil Liberties Union, March 8, 2017, https://www.aclu.org/news/aclu-challenges-warrant-search-data-facebook-page-group-protesting-dakota-access-pipeline

190 "Warrant served on Facebook is overbroad and violates first and fourth amendments, ACLU argues in court filing," American Civil Liberties Union, March 8, 2017, https://www.aclu.org/news/aclu-challenges-warrant-search-data-facebook-page-group-protesting-dakota-access-pipeline

191 "Whatcom County drops warrant for Facebook data on pipeline protest," *The Bellingham Herald*, " March 14, 2017, http://www.bellinghamherald.com/news/local/article138382643.html

192 http://www.npr.org/sections/thetwo-way/2017/04/07/523022497/twitter-withdraws-lawsuit-after-dhs-drops-demands-for-alt-accounts-identity

193 "ADL Report: Anti-Semitic Targeting of Journalists During the 2016 Presidential Campaign," Anti-Defamation League, October 19, 2016, https://www.adl.org/sites/default/files/documents/assets/pdf/press-center/CR_4862_Journalism-Task-Force_v2.pdf

194 Carlett Spike and Pete Vernon, " ' It was super graphic:' Reporters reveal stories of online harassment," *Columbia Journalism Review*, July 28, 2017, , https://www.cjr.org/covering_trump/journalists-harassment-trump.php

interfering with police activities. Covert filming may fall under illegal wiretapping regulations.[195] In July 2016, police briefly detained or harassed individuals who shared footage online of the fatal shootings by police of Alton Sterling in Baton Rouge, Louisiana and Philando Castile in St. Anthony, Minnesota.[196]

## Technical Attacks

Americans witnessed several major cyberattacks on U.S. political organizations and commercial websites in the latter half of 2016, including a hack into the network of the Democratic National Committee (DNC) that played a significant role in media coverage of the 2016 presidential election. In June 2016, the *Washington Post* reported that Russian hackers had gained access to the DNC networks and had obtained opposition research on Donald Trump as well as DNC staffers' email communications.[197] The Kremlin denied any involvement in the hacks.[198] On July 22, days before the Democratic National Convention, WikiLeaks released a trove of emails taken from the DNC server that revealed potentially embarrassing and unfavorable information about the internal workings of the Democratic Party, including DNC conversations about ways to weaken then-Democratic candidate Bernie Sanders.[199] As a result, DNC chairwoman Debbie Wasserman Schultz was forced to resign on the eve of the convention.[200]

During the month of October, WikiLeaks released more documents and email communications obtained from the email account of John Podesta, chairman of the Hillary Clinton campaign, including transcripts of a speech Clinton had made to Goldman Sachs that she had previously refused to make public.[201] In December, President Obama blamed the Russian government for attempting to interfere in the election and retaliated by imposing sanctions on two Russian intelligence agencies.[202] This hacking incident, which started in 2015 and was revealed in mid-2016, was part of a broader set of allegations of Russian government interference in the 2016 U.S. presidential election (see "Media, Diversity, and Content Manipulation").

Commercial websites were also subjected to cyberattacks during the coverage period. A massive DDoS attack against a DNS provider, Dyn, was launched on October 21, 2016 and disabled numerous popular websites for users in the United States and parts of Europe. The DDoS attack was orchestrated through the creation of a "botnet"—in this case, a network of unsecured Internet

195 Dia Kayyali, "Want to Record the Cops? Know Your Rights," Electronic Frontier Foundation, April 16, 2015, https://www.eff.org/deeplinks/2015/04/want-record-cops-know-your-rights

196 PEN America, "Retaliation For Documenting Police," petition, September 12, 2016, https://pen.org/blog/retaliation-documenting-police

197 Ellen Nakashima, "Russian government hackers penetrated DNC, stole opposition research on Trump," *Washington Post*, June 14, 2016.

198 Andrew Roth, "Russia denies DNC hack and says maybe someone 'forgot the password,'" *The Washington Post*, June 15, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/russias-unusual-response-to-charges-it-hacked-research-on-trump/?utm_term=.6e5739865f09

199 Tom Hamburger and Karen Tumulty, "WikiLeaks releases thousands of document about Clinton and internal deliberations," *Washington Post*, July 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.bb1c92b80a33

200 Anne Gearan, Philip Rucker, and Abby Phillip, "DNC chairwoman will resign in aftermath of committee email controversy," *The Washington Post*, July 24, 2016, https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html?utm_term=.3c66f65863a1

201 http://www.cnn.com/2016/10/15/politics/wikileaks-hillary-clinton-goldman-sachs-speeches/

202 David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html

of Things devices infected with malware and used to perpetrate an attack—to flood the Dyn server with requests, causing it to fail.[203] The attack affected websites such as Netflix, Twitter, Amazon, and PayPal.[204]

Financial, commercial, and governmental agencies in the United States have been and continue to be targets of significant cyberattacks. In June 2015, for example, government officials reported two successive cyberattacks beginning in March 2014 which resulted in hackers breaching the Office of Personal Management (OPM) and other executive agencies.[205] The social security numbers of over 21.5 million individuals were stolen from government databases.[206]

In response to these incidents and others, the U.S. has taken a series of legal and policy measures to address growing cyber threats. On May 11, 2017, President Trump issued an executive order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which holds government agency heads accountable for securing the IT infrastructure of their department, and promotes sharing IT resources across agencies in order to secure a "more resilient executive branch IT architecture."[207]

In December 2015, President Obama signed an omnibus bill that included a version of the Cybersecurity Information Sharing Act (CISA) already passed in the Senate. The law requires the Department of Homeland Security to share information about threats with private companies, and allows companies to voluntarily disclose information to federal agencies without fear of being sued for violating user privacy.[208] Civil liberties advocates said that the final text of the bill did not include strong enough privacy protections, and weakened requirements found in earlier drafts to remove from disclosures any personal information not needed to identify cybersecurity threats. Critics also said that allowing companies to voluntarily disclose data to any federal agency—including the Department of Defense and the NSA—undermines civilian control of cybersecurity programs and would blur the line between the use of this data for cybersecurity versus law enforcement purposes.[209]

203 Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind, experts say," *The Guardian*, October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

204 Berkeley Lovelace Jr., and Antonio Jose Vielma, "Friday's third cyberattack on Dyn 'has been resolved,' company says," CNBC, October 21, 2016, http://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html

205 Lily Hay Newman, "Government Discovered Employee Data Breach While It Was Trying to Upgrade Security," *Slate,* June 5, 2015, http://www.slate.com/blogs/future_tense/2015/06/05/office_of_personnel_management_discovered_hack_while_trying_to_upgrade_security.html

206 Brian Naylor, "OPM: 21.5 Million Social Security Numbers Stolen From Government Computers," NPR, July 9, 2015, http://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers

207 Executive Order No. 13800, CFR Vol. 82, No. 93, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf

208 Consolidated Appropriations Act, 2016, Pub. L. 114-113, December 18, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2029/text

209 Jadzia Butler, Greg Nojeim, "Cybersecurity Information Sharing in the 'Ominous' Budget Bill: A Setback for Privacy," Center for Democracy and Technology, December 17, 2015, https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/