JAPAN

Political speech was constrained online for 12 days before the December 2012 election under a law banning parties from campaigning online (see LIMITS ON CONTENT).

In April 2013, the legislature overturned that law, but kept restrictions on campaign emails (see VIOLATIONS OF USER RIGHTS).

2012 amendments to the Copyright Law criminalized intentionally downloading pirated content, though lawyers called for civil penalties (see VIOLATIONS OF USER RIGHTS).

Anti-Korean and anti-Chinese hate speech proliferated online amid real-world territorial disputes (see VIOLATIONS OF USER RIGHTS).

A constitutional revision promoted by the newly-elected LDP party threatens to erode freedoms and rights that “violate public order” (see VIOLATIONS OF USER RIGHTS).

**KEY DEVELOPMENTS: MAY 2012 – APRIL 2013**

- Political speech was constrained online for 12 days before the December 2012 election under a law banning parties from campaigning online (see LIMITS ON CONTENT).
- In April 2013, the legislature overturned that law, but kept restrictions on campaign emails (see VIOLATIONS OF USER RIGHTS).
- 2012 amendments to the Copyright Law criminalized intentionally downloading pirated content, though lawyers called for civil penalties (see VIOLATIONS OF USER RIGHTS).
- Anti-Korean and anti-Chinese hate speech proliferated online amid real-world territorial disputes (see VIOLATIONS OF USER RIGHTS).
- A constitutional revision promoted by the newly-elected LDP party threatens to erode freedoms and rights that “violate public order” (see VIOLATIONS OF USER RIGHTS).
Internet and digital media freedom are generally well established in Japan, where the constitution protects all forms of speech and prohibits censorship. Given this broad lack of restrictions, however, some legislation disproportionately penalizes specific online activities.

Businesses started to recognize the potential of the internet after 1996, when major companies such as Nippon Telegraph and Telephone Corporation (NTT) and Fujitsu offered ISP services. In the early 2000s, providers introduced high-speed broadband. The world’s first large-scale mobile internet service, iMode, was pioneered in 1999 by the nation’s largest mobile carrier, NTT DoCoMo. Today, the internet is a major part of social infrastructure with 79 percent penetration.

Japan’s internet industry is characterized by voluntary self-regulation. The government, especially the Ministry of Internal Affairs and Communications, maintains a hands-off approach when it comes to online content. Law enforcement agencies tend to push for stronger official regulation, and sometimes make arrests based on online activity. Police made a misguided attempt to reign in the chaotic discussion site 2channel in 2012, briefly charging its founder with abetting a drug dealer who had posted a message, but later backed off. Four others, including a student, were detained for several days in July 2012 when police believed them responsible for terror threats sent after malware commandeered their computers.

Japan’s lawmakers also struggle to balance freedom with protection online, with mixed success. A revised copyright law in effect since October 2012 criminalized the deliberate download of a single pirated file; an offence now punishable with jail time. The law already threatens uploaders with up to 10 years in jail—making the commercial distribution of illegally copied entertainment in Japan subject to heavier sentences than the commercial distribution of child pornography.1

Other developments were more positive, particularly a change to restrictions on political speech on the internet that took place in April 2013. In December 2012, politicians stopped using the web for 12 days prior to the general election, which brought the conservative Liberal Democratic Party to power, following an outdated law against online campaigning. Four months after the social-media savvy Shinzo Abe assumed office as prime minister on December 26, the ban was reversed, though confusing limits remain on campaign emails and advertising.2

Troublingly, Abe’s social networking expertise shows signs of turning manipulative, and his rhetoric against neighboring South Korea and China is echoed in increasingly xenophobic online discourse, which in turn fuels right-wing demonstrations. At the same time, the LDP is seeking to change the very core of Japan’s free speech protections by revising the constitution so that rights

---

1 Downloading and viewing child pornography for personal, non-commercial use is legal. A draft law criminalizing possession of child pornography has been in the pipeline since 2009 yet most opposition parties do not support the current language.
“shall not violate public interest”—a disturbing change of emphasis. A national referendum must still approve constitutional revisions. So far, however, Abe’s nationalism has attracted some popular support, to the possible detriment of the online space.

**OBSTACLES TO ACCESS**

In general, Japanese people experience few obstacles to internet access, with penetration at 79 percent in 2012. In late 2011, official figures measured household penetration at 86 percent, and 99 percent for businesses with over 100 employees.

Among individuals, figures show that 79 percent used a home computer to access the internet. Another 66 percent used mobile phones, and another 20 percent used smartphones. Game consoles, tablets, and internet-capable TV amounted to less than 10 percent of usage each. Few still use dial-up connections in Japan, since 60 percent have fiber-to-the-home broadband, according to 2013 government figures. Access is high quality with competitive speeds. In April 2013, So-net, an ISP backed by Sony, said it was launching the world’s fastest internet service for home use in Japan.

The average cost of internet access is around 5,000 yen ($50) per month, though many providers bundle digital media subscriptions, Voice over IP (VoIP) and e-mail addresses, pushing expenses higher. While this remains within reach of most, declining average incomes make staying connected increasingly costly, especially for the younger generation.

NTT, formerly a state monopoly, was privatized in 1985 and reorganized in 1999 under a law promoting functional separation between the company’s mobile, fixed-line, and internet services. Asymmetric regulation, which creates stricter rules for carriers with higher market share, helped diversify the industry, though critics say the expense of switching providers—and the inconvenience of losing an email address and other services—ties customers to the dominant players and creates a barrier for new entrants. While the telecommunications market looks open,

---

7 Informal Freedom House survey of providers’ costs, 2013.
8 The average monthly income for working households in 2010 was 700 yen (US$7) less than it was in 1990. See, Ministry of Internal Affairs and Communications, “Average Monthly Income and Expenditure per Household (Workers) 1955-2010,” Statistics Bureau, [http://www.stat.go.jp/data/chouki/zuhyou/20-06.xls](http://www.stat.go.jp/data/chouki/zuhyou/20-06.xls).
therefore, with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice. No major foreign operators have successfully penetrated the telecommunications market, with the exception of smartphone devices manufactured by Apple and Samsung, though many invest in, or partner with local providers.

Mobile penetration reached 109 percent in 2012. Almost every mobile phone uses packet-based Internet services which helped mobile internet use became popular in Japan even before the introduction of the smartphones, though increasing smartphone use has made the market more competitive. The three major carriers are KDDI Au, NTT DoCoMo and Softbank. According to data published in 2013, the average household in Japan spends around 6,714 yen ($67) for mobile service.

The vulnerability of Japan’s communication network became apparent in March 2011, when an earthquake and tsunami hit Japan’s east coast and caused a nuclear disaster. Infrastructure was severely damaged, leaving many people without service for periods from a few days to one month, and restricting relief efforts. Mobile phone usage dropped by almost half in the affected areas.

Network congestion and server outages—the result of increasing smartphone traffic due in part to many applications sending automatic signals every minute—also frequently affect mobile use. KDDI, one of three major mobile carriers, reported large scale disruptions in December 2012, and January and April 2013. NTT DoCoMo also dealt with four interruptions in July and August in 2012 alone.

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved in the past twelve years under the Ministry of Internal Affairs and Communications (MIC), which regulates the telecommunications, internet, and broadcast sectors. Non-governmental, non-profit organizations supported by the relevant companies in the sector have been formed to self-regulate the industry. These include the television Broadcasting Ethics & Program Improvement Organization, the Content Evaluation and Monitoring Association for mobile platforms, and the Internet Content Safety Association, which manages blocking of child pornography online.

---

15 Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, and before that, the Diet.
Restrictions that undermined internet freedom for 12 days before December 2012 election were lifted the following April. Abe and his supporters were particularly active on digital platforms. Unfortunately, nationalistic discourse lead to vitriolic hate speech directed at South Korean and Chinese communities in some internet forums. The 2011 earthquake continued to cast a long shadow online, as internet journalists not affiliated with traditional media outlets struggled to gain recognition allowing them to cover the aftermath of the nuclear disaster and related protests.

No direct political censorship has been documented in Japan. However, political speech was constrained online in the days preceding the December 2012 election under a law banning parties from using the internet in the run-up to polling. Although the law dated from 1950, it was used to stop politicians from blogging and tweeting during designated campaign periods. In 2012, many retroactively deleted content posted before the campaign formally commenced on December 3rd. Occasional violations led to a warning from the MIC, but no penalties or administrative deletions were reported as a result of the ban, and other candidates flouted or creatively avoided it without repercussions. In April 2013, the restriction was lifted across digital platforms—though some limits on email and advertising remain—in part because Prime Minister Abe has hundreds of thousands of followers on Facebook, Twitter and local network LINE. Conservative politicians had previously resisted such a revision in the past for fear it would empower their opponents.

ISPs voluntarily filter child pornography, and many offer parents the option to filter other immoral content to protect young internet users. Depictions of genitalia are pixelated to obscure them for internet users based on a common—though poorly-articulated—interpretation of article 175 of the penal code, which governs obscenity. Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content. A police Internet Hotline Center which cooperates with ISPs to solicit reports of illegal or harmful content from the public said it received 196,474 calls in 2012. Among them, 20 percent involved illegal content and 75 percent involved obscene material. Providers are not obliged to comply but most cooperate. A few, like 2channel, notoriously refuse.

---

20 Arianna Huffington, “Postcard From Japan.”
The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern take-down requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement. In 2002, industry associations produced guidelines designed to protect ISPs from legal liability within the jurisdiction of the Japanese courts. Under the guidelines, anyone can report material that infringes directly on their personal rights to the service provider, either to have it removed or to find out who posted it. No third party can do so. The provider notifies the individual who posted the content, and either fulfills the request with their permission or removes the content without the authors’ approval if they fail to respond within two weeks. If the poster refuses permission, the service provider is authorized to assess the complaint for themselves, and comply if they believe it is legitimate. In this scenario, an ISP could give the complainant information to identify the poster—such as their name or IP address—without that person’s consent, leading to privacy concerns. This process is voluntary, but by complying, service providers protect themselves from civil liability. In practice, many citizens say service providers have failed to remove libelous content.

Police sometimes intervene more directly, and their emphasis on security over transparency occasionally threatens internet freedom. In April 2013, they recommended ISPs and website administrators cooperate to block IP addresses used by Tor—which allows internet users to disguise their location by connecting through a network of other computers—in order to prevent criminals from abusing the service, which also has many legitimate applications.

The threat of official content restrictions looms periodically during public debates about child safety, though carriers and content producers have successfully resisted intrusive regulation. In 2007, the MIC ordered mobile operators to install filtering software enabling parents to control content seen by their children. A coalition of groups, including the Japan Internet Providers Association and the user rights organization Movement of Internet Active Users lobbied against the mandate, and mobile users can now select voluntary filters. Complaints to the official Consumer Affairs Agency about quasi-gambling functions in games played by children on mobile devices shot up in 2011, along with calls for government regulation. In 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors instead. Games integrated with social networks have also been criticized for their potential for abuse by sexual predators.

Private interests also pressure ISPs to restrict content. In June 2012, a coalition of music rights advocates were reportedly offering to sell service providers a tool to detect whether material being uploaded to the internet is subject to copyright, and sever connections of users violating Japan’s strict copyright laws.\(^{31}\) None are known to have purchased it.

Japanese citizens exercise some self-censorship online, often on historical and social issues. The society at large prefers “harmony,” and people avoid criticizing the role of Japan’s Emperor, especially when connected with historic issues like World War II. Individuals and public figures who break this code risk censure and even attacks from right-wing fanatics, who notoriously tried to assassinate the Nagasaki mayor on these grounds in the 1990s. Though exceptional, incidents like this still exert a chilling effect on Japanese expression.

There are few known cases of the government or powerful groups proactively manipulating online news or other content. In a significant exception, officials and the Tokyo Electric Power Company withheld data about pollution after a nuclear power plant in Fukushima prefecture was severely damaged by the 2011 earthquake and tsunami, and citizens unwittingly exposed themselves to radiation. The MIC requested that four industry associations monitor false or unsubstantiated content circulating about the disaster online, including on social networks. Some observers said this was a measure to control public discourse, though deletions were not widespread. Service providers removed content, which included images of corpses, in at least 13 cases,\(^{32}\) though the national police agency reported 41 items for review.\(^{33}\)

The disaster also had an impact on social media use. YouTube, Twitter, and international blog-hosting services are freely available, as are popular domestic platforms like Nico Nico Douga, a video-sharing site, and LINE, a chat application launched in 2011. Facebook recently overtook domestic rival Mixi, more than doubling its Japanese customer base between May 2011 and May 2012, as many users sought to connect with loved ones and exchange news on a single platform.\(^{34}\) The earthquake also spurred cloud funding of civic causes,\(^{35}\) and the launch of Twitter’s Lifeline feature, which lists government accounts providing public information in emergencies, in September 2012.\(^{36}\)

---

Though slowed by the aforementioned online campaigning restriction, many politicians are embracing digital tools. Toru Hashimoto, the governor of Osaka, has more than one million followers on his Twitter account @t_ishin, while the governor of Tokyo, Naose Inoki’s account @inosenaoki has over 300,000. Both are popular for calling out their critics by name, including reporters and politicians. However, some news reports from the past year expressed concern about manipulated online discourse. In December 2012, the prime minister’s secretary invited his Facebook supporters to bombard a public broadcaster with messages of support in advance of a scheduled panel appearance she assured them would include “Abe-bashing,” Abe subsequently updated the account himself to belittle his opponents on the panel.37

These interventions are more significant in the context of escalating online hate speech targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments. Abe’s stance on these active rivalries, as well as historic ones, does nothing to calm the situation. In December 2012, he said he was reconsidering apologies Japan had made for acts of wartime aggression, including one for forcing Asian and European women to work in army brothels, which he denied was coerced. While he later retracted this position,38 an advertisement with a government seal that appeared to support such a revisionist history was widely circulated on social media in early 2013, though it turned out to be fake.39 The incitements to violence directed at South Korean and Chinese people—and unpatriotic activity in general—which flourished on websites like 2channel in the past year, were far more extreme, but they were arguably rooted in the same nationalist discourse, which threatens to undermine the diversity of voices being heard in Japanese cyberspace.40

Blogs have a significant impact on public opinion, and several independent journalists are becoming influential through personal or commercial websites and social media accounts. Yet most online media remain small and community-based, with no major national successes, and the mainstream media’s habit of compliance and restraint may be standing in the way of the combative online news culture flourishing elsewhere in Asia.41 Kisha clubs, formal organizations only open to traditional media companies, and an advertising market that favors established players, may be preventing digital media from gaining a foothold in the market. Kisha clubs provide essential access to officials in Japan, but discriminate against new media practitioners. At least one online journalist was denied access to one of their Tokyo locations in October 2012.42 The previous May, the only two freelancers permitted to join an official group of 40 reporters on a tour of the nuclear disaster site

40 Tessa Morris-Suzuki, “Freedom of Hate Speech.”
were forbidden from taking equipment. In the meantime, independent online news outlets have struggled to sustain themselves financially. OhmyNews, a South Korean platform, established a Japanese operation in 2006, but closed in 2008. The US-based Huffington Post digital media website launched a Japanese-language version in May 2013.

A number of civil liberty groups are actively engaged in the online space. Movements for the Internet Active Users, founded by activist Daisuke Tsuda and 11 colleagues in 2007, is one example, a user rights group that contests excessive content regulation and advocates for free speech.

**VIOLATIONS OF USER RIGHTS**

The strong protections in Japan’s constitution were potentially put in jeopardy in 2012, after the now-incumbent LDP party proposed making them subject to limits to protect public order. While their reversal of a ban on internet campaigning was positive, the law retained disproportionate penalties for violating email restrictions to solicit political support, including possible jail terms. An already-strict copyright law was also strengthened during the coverage period to criminalize downloading illegal material. Public trust in the police implementing these laws was undermined when they charged an online entrepreneur for abetting a criminal, saying the bulletin board he founded failed to delete a post offering drugs for sale, and jailed four people for nearly a month on charge of sending threatening messages, though all proved to be innocent.

Article 21 of Japan’s constitution prohibits censorship and protects freedom of “speech, press and all other forms of expression,” as well as the “secrecy of any means of communication.” In general, individuals and media can exercise this in practice, though social and legal constraints exist.

In May 2012, the LDP, then in the opposition, proposed revising the constitution. In December, the party gained a landslide electoral victory in the Diet, the lower house; they went on to win the senate in July 2013. Critics say their draft promotes conservative nationalism, replacing the subject of the constitution—currently the people of Japan—with the nation state. While it would not affect the protections outlined above, it does add that “freedoms and rights come with

---


responsibilities and duties, and shall not violate public interest and public order.” A national referendum must still approve the revision, which would also lower the bar for making future constitutional changes.

A more positive LDP initiative undid long-standing restrictions on use of the internet for election campaigns for the first time in 2013, and a revision of Public Offices Election Act passed the Upper House on April 19. Limits remained on paid online advertising and campaign emails, which could only be sent directly by a party or candidate—not a supporter—in a measure designed to prevent fraud, though members of the electorate can freely solicit support on social media.50 While these provisions were contested and revisions are still planned,51 news reports during the coverage period said politicians violating these restrictions face a potential 300,000 yen ($3,060) fine or one year in prison; imprisonment would strip them of political rights to vote or run for office. Voters found improperly soliciting support for a candidate via e-mail could be fined 500,000 yen ($5,100) or jailed for two years, which would also deprive them of political rights.52

Another legal revision passed during the coverage period of this report introduced potentially disproportionate sentences for copyright violators—including any internet user downloading content they know has been illegally copied, as opposed to those engaged in piracy for commercial gain.53 While both uploading and downloading pirated material was already illegal under the copyright law, with uploaders subject to 10 years imprisonment or fines up to 10 million yen ($102,000), the version in effect since October 1, 2012 added two years in jail or fines up to two million yen ($20,500) for downloading a single file.54 The Japanese Bar Association said that downloading, as an essentially insignificant personal act, should be regulated by civil, instead of criminal laws.55 Police launched a nationwide antipiracy crackdown, searching 124 different locations and arresting 27 people under the law in February 2013.56

The sentences for copyright and e-mail fraud seem particularly harsh in light of Japan’s lack of restrictions on child pornography and hate speech online, which are acceptable to limit under international law.57 Laws passed in 1999 and 2003 outlawed the production, distribution and sale of

---

hardcore child pornography, including electronically, but possessing it for non-commercial use remains legal except in Kyoto prefecture, central Japan, where police arrested three people for purchasing child pornography online for the first time in September 2012 under an ordinance in effect since the previous January. Although nationalistic hate speech and incitement to racially-motivated violence is proliferating online, the government has taken no action to curb it on grounds it is already criminalized under the penal code; yet police in 2012 were more likely to use the relevant clauses to prosecute antinuclear demonstrators than groups whose on and offline slogans included exhortations to “kill Koreans.”

Article 175 of the Japanese penal code bans the sale or distribution of broader categories of obscene material, and while it dates from over 100 years ago, it is considered to apply online. However, it does not define what constitutes obscenity, leading to concerns that it may infringe on artistic expression and LGBT rights.

No citizens have faced politically motivated arrest or prosecution for content they have published online, though observers believe that police sometimes overstep during cybercrime investigations. Four people, including a student, were detained for nearly a month in July 2012 for sending electronic terrorism threats that had actually been triggered without their knowledge, by malware. In November 2012, police charged 2channel founder Hiroyuki Nishimura with abetting the drug trade, saying he failed to delete a post from someone trading amphetamines on the rambunctious bulletin board; the allegation was complicated by the fact that Nishimura no longer manages the site, and was dropped without explanation in March. Police were less diligent in another case, however. On November 6, 2012, a woman in Kanagawa prefecture was stabbed and killed by a stalker police had refused to investigate in March, when she reported him for sending over 1000 threatening emails in 20 days—in part because the law governing stalking does not explicitly ban harassment via email. A bill to establish an independent human rights commission

---

60 Tessa Morris-Suzuki, “Freedom of Hate Speech.”
which may address online abuses like cyberbullying was announced in September 2012, but the
details and possible timeframe involved remain unclear.67

Japan’s Supreme Court protects privacy through its interpretation of Article 13 of the constitution,
which provides for the right to life and liberty,68 while 2003 laws specifically protect personal data
amounting to more than 5,000 records collected electronically by both the private and the public
sector.69 Law enforcement requests for this data should be supported by a warrant, though some
cooperate without one.70 Individuals may be afforded less due process. In November 2012, police
raided the home of Yuzuru Kaneko, who documented antinuclear protests on YouTube, seizing his
footage and equipment in an attempt to prove wrongdoing by one of the protesters.71

Under voluntary guidelines drafted by four ISPs in 2005, service providers automatically inform
police of internet users identified on pro-suicide websites, and comply with law enforcement
requests for information related to acts of self-harm.72

Through the Resident Basic Register Network System in effect for over a decade, Japanese citizens’
unique ID numbers are stored in a national juki-net computer network which critics say is
vulnerable to cyberattacks, although this risk is partially offset by the fact that it has no centralized
database.73 Some individuals and municipalities have refused to participate in the database.74 A “My
Number Bill” proposed by the cabinet in 2012 would potentially increase the kinds of personal data
government agencies would collect and share electronically, a measure the Japanese Bar Association
and other groups oppose for threatening privacy.75

“Secrecy of communication” is protected under telecommunications laws,76 and there are no
restrictions on anonymous online speech except in internet cafes, where users are required to
produce formal ID such as a driver’s license and register their name and address. Police can request
these details, along with usage logs, if they detect illegal online activity. A law enacted in 2003 and

68 Privacy International, “Chapter i: Legal Framework,” in Japan, December 12, 2006,
70 Privacy International, “Chapter iii: Privacy Issues,” in Japan, December 12, 2006,
71 Keiko Tanaka, “Police Raid Video Blogger’s Home in Japan,” November 15, 2012,
73 Rebecca Bowe, “In Japan, National ID Proposal Spurs Privacy Concerns,” Electronic Frontier Foundation, June 13, 2012,
Number System’ Bill,” February 15, 2012,
76 Ministry of Internal Affairs and Communications, “Telecommunications Business Act,” December 25, 1984,
revised in 2008 prohibits electronic communications encouraging sexual activity with minors.\(^{77}\) Under the law, all online dating services must register with police, verify their customers’ ages with a driver’s license or credit card, and delete or block content that appears to involve someone under 18; most services voluntarily monitor messages in real time to ensure compliance.

Under a wiretap law enacted in 1999, law enforcement agents may seek a court order to conduct electronic surveillance in criminal investigations involving drugs, firearms, human trafficking, or organized murders, an exception to articles of other laws that explicitly forbid wiretapping.\(^{78}\) The law obliges agents to notify targets of wiretaps after investigations are concluded and inform the Diet about the number they implement annually. While the law was extremely controversial when it passed, in part due to the authorities’ politicized abuse of surveillance in the recent past,\(^{79}\) lawmakers were seeking to expand it in December 2012.\(^{80}\) Critics say the law does not prevent the systematic storage of intercepted communications or protect innocent parties.\(^{81}\) Security agents and the military have been accused of implementing surveillance in cases involving national security.\(^{82}\)

No physical violence has been reported against bloggers or internet users in relation to their online activity. While distributed denial-of-service (DDoS) attacks were part of the arsenal used by nationalists in Japan, China and South Korea to target perceived opponents in other countries, and cyberattacks have been reported against commercial and government targets,\(^{83}\) they are not known to have been used to systematically target individuals or civil society groups. In acts of protest against the copyright law, hackers briefly targeted websites of several political parties and institutions in October 2012.\(^{84}\)

---


\(^{81}\) Privacy International, “Chapter ii: Surveillance.”

