Freedom House

Japan

	2014	2015
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	7	7
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**22**	**22**

* 0=most free, 100=least free

Population:	**127 million**
Internet Penetration 2014:	**91 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2015 Status:	**Free**

Key Developments: June 2014 – May 2015

- Courts upheld users' "right to be forgotten" in Japan, requiring search engine companies to delete links to material at the user's request in specific cases (see **Content Removal**).
- Despite privacy concerns, the rollout of the "My Number" national resident registry system is scheduled for late 2015 and early 2016 (see **Surveillance, Privacy, and Anonymity**).
- Telecommunications companies eased restrictions on third-party SIM cards that observers feared had been limiting users' ability to switch carriers (see **ICT Market**).

Introduction

As in past years, privacy concerns, data leaks, and cyberattacks were key issues for Japanese internet users during the coverage period. Japan's constitution protects all forms of speech and prohibits censorship, while the government, especially the Ministry of Internal Affairs and Communications, maintains a hands-off approach to online content, which is generally regulated voluntarily by industry players. Internet penetration is over 90 percent. Despite strong access, however, some legislation disproportionately penalizes specific online activities.

As part of the Abe administration's strategy to boost national security, lawmakers passed the Act on the Protection of Specially Designated Secrets in 2013. The legislation, which criminalized both leaking and publishing broadly defined national secrets regardless of intent or content, has repercussions for journalists, whistleblowers, and civil society watchdogs, particularly in the age of the internet. In a review of Japan's human rights practices in July 2014, the United Nations Human Rights Committee said the legislation laid out "a vague and broad definition of the matters that can be classified as secret" and "high criminal penalties that could generate a chilling effect on the activities of journalists and human rights defenders."[1]

Attention to data security also escalated in 2014, with the high-profile arrest and trial of an engineer for leaking personal data belonging to customers of the Benesse educational services corporation. In Japan's largest data leak to date, Benesse confirmed "the leak of personal data of at least 7.6 million people [noting that]...the problem could ultimately affect more than 20 million."[2]

Such attention to security measures is of particular concern for national and local governments as they gear up for the introduction of the "My Number" system of personal ID numbers throughout the country.[3] Amendments to the Act on the Protection of Personal Information to strengthen data privacy penalties to remove personal information that identifies individuals were passed in the Diet in early September 2015.[4] Such amendments may also forestall fears of possible data leakages with the rollout of the "My Number" system in October 2015.[5]

1 United Nations International Covenant on Civil and Political Rights Human Rights Committee, "Concluding observations on the sixth periodic report of Japan," August 20, 2014, available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fJPN%2fCO%2f6&Lang=en.

2 "1,789 file Y100 mil damages suit against Benesse over data leak," *Japan Today*, January 29, 2015, http://bit.ly/1L1MOBP.

3 "Gov't should give up use of 'My Number' system infringing on people's human rights," *Japan Press Weekly*, February 25, 2015, http://bit.ly/1jQN0eh; Ryo Asayama, "Japan's 'My Number' system offers IT boon, and risk," *Nikkei Asian Review*, March 17, 2015, http://s.nikkei.com/1Lorvrl.

4 "Revised personal information protection law enacted," *Mainichi Shimbun*, September 4, 2015.

5 "マイナンバー法案が審議入り　衆院本会議," [My Number Law proposal enters committee, Lower House plenary session] *Nikkei Asian Review,* April 23, 2015, http://s.nikkei.com/1L1MX8r; "マイナンバー法改正案が衆院可決　貯金口座にも適用,"[My Number Law amendments expected to pass in the Lower House, will be applied to savings accounts] ITmedia, May 21, 2015, http://bit.ly/1VH275Y ; "マイナンバー衆院通過　貯金口座にも適用　個人情報保護法改正案も," [My Number Law passes in the Lower House, to be applied to savings accounts, proposed amendments to Personal Privacy Law as well] *Sankei,* May 21, 2015, http://bit.ly/1c7UmFR.

Obstacles to Access

In general, Japanese internet users experience few obstacles to access. Internet access remains high, and mobile phone companies are increasing reaching out through expanded technological offerings. One major development in the past year has been the availability of third-party SIM cards with mobile operators unlocking phones for a small fee, and the greater availability of SIM-free models of phones and tablets.

Availability and Ease of Access

Internet penetration was at 91 percent in 2014, up from 90 in 2013.[6] Mobile phone penetration reached 120 percent in 2014.[7] Official statistics report slightly over 155 million mobile phones (including personal handy-phone systems, or PHS) in use in Japan as of March 31, 2015, equivalent to a penetration rate of 121.1 percent and demonstrating an increase of 4.9 percent over the previous year's figure.[8] Access is high quality with competitive speeds averaging 15.2 Mbps in early 2015.[9]

The average cost of internet access is around JPY 5,000 (US$50) per month,[10] though many providers bundle digital media subscriptions, Voice over IP (VoIP), and email addresses, pushing expenses higher. While this remains within reach of most, declining average incomes make staying connected increasingly costly, especially for the younger generation.[11] According to data published in 2013, the average household in Japan spends around JPY 6,925 (US$69) for mobile service per month, or JPY 83,099 yen (US$830) per year.[12] The private Wire & Wireless service offers free Wi-Fi access in restaurants, coffee shops, and some train stations; registration requires an email address.[13]

As these figures suggest, access is well distributed across the population, though less common among the elderly. According to the MIC Information Communications Statistics Database, internet penetration was 72 percent for children aged 6 to 12, and over 95 percent in the age ranges of 13 to 49, compared to 21 percent for people over 80 years of age.[14] Mobile phone operators are expanding their market for handsets designed for children and for the elderly, with easy-to-use, large-button phones.

Restrictions on Connectivity

There are few infrastructural limitations on internet access in Japan, though the vulnerability of

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

7 International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2013," http://bit.ly/1cblxxY.

8 Ministry of Internal Affairs and Communications, "Information and communications statistical database, basic data" [in Japanese], http://bit.ly/1ZgX2FO.

9 Akamai's *State of the Internet*, "Asia-Pacific Highlights (Q1, 2015)," June 24, 2015, https://www.stateoftheinternet.com/resources-connectivity-2015-q1-state-of-the-internet-report.html.

10 Informal Freedom House survey of providers' costs.

11 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 Statistics Bureau, "Average Monthly Income and Expenditure per Household (Workers) 1955-2010," http://www.stat.go.jp/data/chouki/zuhyou/20-06.xls.

12 Ministry of Internal Affairs and Communications, "White Paper Information and Communications in Japan 2014," [in Japanese] http://bit.ly/1jcW9x8.

13 Starbucks, "at_STARBUCKS_Wi2," http://starbucks.wi2.co.jp/pc/index_en.html.

14 Ministry of Internal Affairs and Communications, Information and Communications Statistics Database, *Heisei 26 nen chosa*, http://bit.ly/1mLIJEl.

Japan's communication network became apparent in 2011, when an earthquake and tsunami hit Japan's east coast, triggering a nuclear plant accident. 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.[15]

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 2012 and 2013. Fewer disturbances were reported during this year's coverage period.

In 2013, Nippon Telegraph and Telephone Corporation's (NTT) Docomo announced an expansion in LTE base stations to augment its Xi LTE and FOMA 3G services.[16] Providers such as Asahi-net offer WiMAX plans with mobile routers capable of accessing multiple networks throughout the country.[17] Historically, Japan's internet connections were forged through cooperation among government agencies (including ministries and NTT, which was a government-owned monopoly until 1985), higher education institutions (mainly national universities), and national research institutions. According to the internet timeline available on the Japan Network Information Center website, the first network operations (known as the "N-1 Network," in operation from October 1974 to December 31, 1999) were a joint undertaking initially operated by the University of Tokyo, the University of Kyoto, and NTT that later expanded to link other national universities in Japan.[18] The network of connected institutions started to expand in the mid-1980s with the start of JUNET (Japan University Network), pioneered by Keio University professor Jun Murai. The first Japanese university to connect to an overseas university was the Tokyo University of Science (connecting with the City University of New York) in 1985.

ICT Market

Japan has three major mobile operators—KDDI Au, NTT Docomo, and Softbank. All use the CDMA wireless network or a variant. 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.[19] Asymmetric regulation, which creates stricter rules for carriers with a higher market share, helped diversify the industry.[20] While the telecommunications market operates with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice.[21] NTT Docomo held close to 40 percent of Japan's mobile market in 2015.[22] No major foreign operators have successfully penetrated the telecommunications market independently; smartphone devices manufactured by Apple and Samsung are available to consum-

15 Izumi Aizu, "The Role of ICTs During the Disaster," *Global Information Society Watch Report 2011,* Association for Progressive Communications, 2011, http://bit.ly/1FZMXGU.

16 NTT DOCOMO, "DOCOMO Introduces Compact LTE Base Station – Downsized Equipment Will Facilitate Wider, Denser LTE Coverage," press release, June 20, 2013, http://bit.ly/1Oo6lyP.

17 AsahiNet, "Asahi Net WiMAX 2+," http://bit.ly/1N1Q6FQ.

18 Japan Network Information Center, "The Internet Timeline," accessed Sept 1, 2015, https://www.nic.ad.jp/timeline/en/.

19 Law Concerning Nippon Telegraph and Telephone Corporation, Etc., No. 85, December 25, 1984, as last amended by Law No. 87, July 26, 2005, http://bit.ly/1FZNyIG.

20 Toshiya Jitsuzumi, "An Analysis of Prerequisites for Japan's Approach to Network Neutrality," (paper, Proceedings of the Telecommunications Policy Research Conference, 2012) http://bit.ly/1dPQDcb.

21 Minoru Sugaya, "Regulation and Competition in the JP Broadband Market," (presentation, Pacific Telecommunications Council, Tokyo, Japan, January 15, 2012) http://bit.ly/16U0HvB.

22 "NTT Docomo bundles mobile and broadband, shaking up sector," *Japan Times*, February 17, 2015, http://bit.ly/1OnS8mQ.

ers through partnerships with the major mobile operators. Consolidation in the mobile industry continued in Japan during this year's coverage period, as Ymobile, which was formed in August 2014 through a merger of Emobile (formerly a roaming mobile company) and Willcomm (a PHS carrier),[23] joined the Softbank group of companies as of April 1, 2015.[24]

Despite this background, increasing smartphone use has made the mobile market more competitive and resulted in improved pricing options: bundling mobile tablet plans with subsidies for second and third devices purchased by consumers; decreases in prices for data and family plans; and the introduction of benefits for long-term customers, such as such as those offered by Docomo to customers with 5- to 15- year histories of continuous service.

In a positive development, third-party SIM card availability increased during the coverage period. In the summer of 2014, the government announced plans to require cellphone carriers to unlock the SIM cards in mobile phones if requested by users, facilitating the use of third-party prepaid SIM cards.[25] In October 2014, the MIC issued new guidelines concerning SIM card unlocking.[26] The new guidelines, which went into effect in May 2015, also stipulate that users must pay outstanding handset costs prior to switching carriers. Though the guidelines were still subject to criticism,[27] they helped address concerns that the cost of switching providers favored the dominant players and created a barrier for new entrants to the market. Besides benefitting Japanese consumers,[28] the change will serve the influx of tourists to Japan anticipated prior to the 2020 Tokyo Olympics.[29]

Regulatory Bodies

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved since the 2001 establishment of the Ministry of Internal Affairs and Communications (MIC), comprised of two former ministries (the Ministry of Home Affairs and the Ministry of Posts and Telecommunications) which were merged with the central government's Management and Coordination Agency. This "super ministry" regulates the telecommunications, internet, and broadcast sectors.[30] Nongovernmental, nonprofit organizations supported by the relevant companies in the sector have been formed to self-regulate the industry. These include television's Broadcasting Ethics & Program Improvement Organization, the Content Evaluation and Monitoring Association for mobile platforms, and the internet's Content Safety Association, which manages blocking of child pornography online.[31]

23 "Ii mobairu to uirukomu ga "Y!mobile" ni – 8-gatsu ni burando o tōgō, sumaho 2 kishu nado shin tanmatsu o junji hatsubai," [E-Mobile and Willcomm merge their brands in August to become 'Y!mobile;' new handsets including two new smartphones to be launched successively] *ITmedia,* July 7, 2014, http://bit.ly/1Qb1Q9Q.

24 SoftBank Corp. , "Notice of Merger," press release, January 23, 2015, http://bit.ly/1Qb21BY.

25 "Japanese cellular carriers to get ministry call to 'unlock' cellphones," *Asahi Shimbun*. June 29, 2014.

26 "New rule to OK unconditional switching of mobile carriers," *Japan Times*, October 1, 2014.

27 "Editorial: SIM lock removal requirement not enough for consumers," *Mainichi Daily News*, November 4, 2014.

28 "Phone users in Japan still paying for plenty of stuff they don't need," *Japan Times*, May 23, 2015.

29 "Narita airport to get SIM card vending machines," *Japan Times*, July 17, 2015.

30 Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, before that, the Diet.

31 Broadcasting Ethics & Program Improvement Organization, "About BPO," http://bit.ly/1jevVLs; Content Evaluation and Monitoring Association, "About EMA," [in Japanese] http://bit.ly/1P0Mqrf; Internet Content Safety Association, "About the Organization," [in Japanese] http://bit.ly/1Mhsnmy.

Limits on Content

Politicians embraced social media for campaign purposes during the 2013 Upper House election after outdated restrictions on digital electioneering were revised during the previous coverage period and continued to expand online campaigning in the December 2014 general election to the Lower House. Activists and civil society also used digital tools to promote local civic causes, and online activity was increasingly effective as a means to combat hate speech and racism.

Blocking and Filtering

No direct political censorship has been documented in Japan. ISPs voluntarily filter child pornography, and many offer parents the option to filter other immoral content to protect young internet users.[32] 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.[33] Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content.

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. [34] 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.[35] Instead, in 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors.[36] 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 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.[37] No follow-up was reported.

Content Removal

Throughout the coverage period, there were a number of cases in Japan involving the "right to be forgotten," a practice allowing users to request that search engines delink material about them from

32 Agence France-Presse, "Japan Internet Providers Block Child Porn," Benton Foundation, April 21, 2011, http://bit.ly/1jQS9Di; Electronic Network Consortium, "Development and Operation of the Next-Generation Rating/Filtering System on the Internet," press release, via New Media Development Association, April 30, 1999, http://www.nmda.or.jp/enc/rating2nd-en.html.

33 Amanda Dobbins, "Obscenity In Japan: Moral Guidance Without Legal Guidance," 2009, http://works.bepress.com/amanda_dobbins/1.

34 Izumi Aizu, "Japan," *Access to Online Information and Knowledge 2009,* Global Information Society Watch, http://bit.ly/16AioGr.

35 Ishaan, "Japanese Social Games Risk Seeing Crackdown," *Siliconera,* May 7, 2012, http://bit.ly/1Mht0fY.

36 Dr. Serkan Toto, "Self-Regulation: Dena Introduces Payment Caps For Minors On Mobage [Social Games]," Kantan Games, Inc (blog), April 24, 2012, http://bit.ly/1MhtfYn.

37 Enigmax, "Jail For File-Sharing Not Enough, Labels Want ISP-Level Spying Regime," *TorrentFreak,* June 24, 2012, http://bit.ly/1L1QnIa.

public results in their country. In October 2014, the Tokyo District Court handed down a provisional order requesting that Google delete half of 237 entries involving a plaintiff's name and subsequently entered text.[38] This incident was noted as possibly the first instance in Japan involving the courts and the removal of search results, and Google Japan stated its willingness to comply with "legal take-down notices."[39] Attention to this issue grew in the following weeks, and in November 2014, Yahoo Japan created an expert panel to investigate the right to be forgotten, with a six-month mandate to examine the situation.[40] At the time, Yahoo Japan also noted that it does not comply with "requests to remove search results except for certain cases involving past crimes," citing the reason that "one company alone cannot decide what society should and should not have access to."[41]

In March 2015, Yahoo Japan unveiled a new set of rules, stating that "it will respond to requests to remove information from search results after weighing privacy protection versus freedom of expression and the right to know…including information such as individuals' personal addresses and telephone numbers."[42] It should be noted that contrary to the EU's sweeping laws concerning the right to be forgotten on the internet, to date there is no similarly broad law in Japan, and cases against search engine companies have been dealt with on an individual basis by each search engine company separately.

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern takedown requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement.[43] 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. 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.[44]

In recent years, content removals have focused on obscene content, including child pornography and "revenge porn," explicit images shared without consent of the subject. After complying with a takedown order in August 2014, Facebook was further ordered by a Tokyo court in October 2014 to "disclose the IP addresses used by fake accounts that were posting revenge porn."[45] A law to address online harassment by means of posting explicit images without the subject's consent passed in November 2014. Prior to this law's passage, upon receiving a complaint, providers were legally obligated to contact the original poster of the images to indicate that such objectionable content would be taken down within seven days. In the case where there was no response from the original poster, the

38 "Tokyo court orders Google to delete data linking man to crime," *Japan Today*, October 11, 2014, http://bit.ly/1Nq5mzA.

39 "Japan court orders Google to delete data," *Sydney Morning Herald*, October 10, 2014, http://bit.ly/1nfzAZQ.

40 "Yahoo Japan to set up expert panel on 'right to be forgotten'," *Mainichi Daily News*, November 8, 2014,

41 "Yahoo Japan considers new policy for removal of search results," *Japan Times*, November 7, 2014.

42 "Yahoo Japan unveils new rules on 'right to be forgotten'," *Mainichi Daily News*, March 31, 2015.

43 Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders, No. 137, November 30, 2001, available at UNESCO, http://bit.ly/1VH6zBu.

44 Business Software Alliance, "Country Report: Japan," 2012, http://bit.ly/1VH7uHq.

45 "Court orders Facebook to reveal revenge porn IP addresses," *Japan Today*, October 22, 2014,

content could be legally deleted by the provider. The new law passed in 2014 reduced the duration of time allowed to the providers to comply with takedown requests from seven days to two days (see Legal Environment).[46] Between November 27 and December 31, 2014, over 100 complaints of revenge porn were received by the National Policy Agency.[47]

The Internet Hotline Center, operated through the Internet Association Japan as part of a contract with the National Police Agency, cooperates with ISPs to solicit reports of illegal or harmful content from the public.[48] While the center received a record high of 196,474 calls in 2012, 150,352 reports were received in 2014.[49] (Over 40,000 reports were received in the first three months of 2015.[50]) The center's breakdown of reports by type reveals 23 percent involved illegal information (information involving illegal activities such as public displays of obscene materials or "publicly inciting or soliciting others to abuse controlled substances") with over 50 percent originating from overseas; 3 percent involved harmful information (information that could invite illegal conduct, related to suicide, or which is "difficult to judge as illegal but seems to be illegal") with 67.5 percent of the cases originating overseas; and 75 percent which "were beyond scope of its operational guidelines, including defamation, slander, murder notices, intellectual property infringement, information inappropriate for children, and other cases."[51] Providers may, but are not obliged to, comply with content removal requests submitted through the center.

Media, Diversity, and Content Manipulation

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 Two. 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,[52] though the National Police

46 "Ribenjiporuno ni chōeki 3 nen ika no bassoku jimin hōan teishutsu e" ("LDP submit Bill to punish revenue porn with up to three years' imprisonment"), *Nihon Keizai Shimbun*, October 12, 2014. (http://www.nikkei.com/article/DGXLASFS11H03_S4A011C1PE8000/)

47 Takuro Yagi, "Police field 110 complaints of 'revenge porn' in first month of tough new law," *Asahi Shimbun*, April 3, 2015.

48 Internet Hotline Center Japan, "Annual Statistics 2013," May 1, 2014, http://www.internethotline.jp/statistics/2013e.pdf.

49 Internet Hotline Center Japan, "Annual Statistics 2014," [in Japanese] http://www.internethotline.jp/statistics/2014.pdf.

50 Internet Hotline Center Japan, "Statistical Information," [in Japanese] 2007-2014, http://www.internethotline.jp/statistics/.

51 Internet Hotline Center Japan, "Annual Statistics 2014."

52 Madeline Earp, "Freelance, online reporting discouraged on nuclear threat," Committee to Protect Journalists (blog), April 14, 2011, https://cpj.org/x/42f5; Ministry of Internal Affairs and Communications, "Demand for Telecommunications Carriers Associations Regarding the Appropriate Response to False Rumors on the Internet Related to the Great East Japan Earthquake,"[in Japanese] press release, April 6, 2011, http://bit.ly/1PjW9It.

Agency reported 41 items for review.[53] Others found an outlet to report on the aftermath of the disaster online.[54]

In 2014, media observers expressed concern that the government had enjoyed undue influence over mass media content when the *Asahi Shimbun* newspaper retracted stories about the "comfort women" forced to work in army brothels during World War Two. The stories, which the paper said relied on one misleading source, had provided support to a revisionist effort to refute women's assertions they were kidnapped and assaulted by Japanese soldiers. Since this position is held by many Abe supporters, readers speculated the inaccurate reports were the product of official "guidance."[55] However, there was no evidence of a direct link between the coverage and Abe's administration, or of political "guidance" influencing online content.

During the 2013-14 coverage period, some news reports expressed concern about nationalistic discourse by Japanese web trolls, or *netōyo,* escalating into hate speech online, particularly targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments.[56] Tensions were high during 2013. In one incident, an advertisement with a government seal that appeared to support revisionist history was widely circulated on social media, though it turned out to be a fake.[57] Nationalist discourse and incitements to violence directed at South Korean and Chinese people also flourished on the internet.[58] However, during the coverage period, a movement to combat hate speech gained ground (see Digital Activism).

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,[59] 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.[60] 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 have been accused of discriminating against new media practitioners in the past. In 2012, at least one online journalist was denied access to one of their Tokyo locations,[61] and the only two freelancers permitted to join an official group of 40 reporters on a tour of the nuclear disaster site were forbidden from taking equipment.[62] Some online news outlets have struggled to sustain themselves financially. *OhmyNews,* a South Korean platform, established a Japanese operation in 2006, but

53 National Police Agency, "For Police Responding to False Rumors on the Internet," [in Japanese] June 21, 2011, http://bit.ly/1VH7lOT.

54 Keiko Tanaka,"20 Bitter Voices Rise From Fukushima After Japan's 2011 Nuclear Disaster," trans. Taylor Cazella, *Global Voices*, December 2, 2013, http://bit.ly/1L90n0j.

55 Philip Brasor, "The highlights of Japanese media in 2014," *Japan Times*, January 3, 2015.

56 Keiko Tanaka, "Countering Hate Speech in Tokyo's Koreatown," trans. Aparna Ray, *Global Voices*, March 6, 2014, http://bit.ly/1Rw5GLE.

57 Keiko Tanaka, "No More Apologies – Japan's Facebook Users Share 'Fake' Propaganda," *Global Voices,* April 19, 2013, http://bit.ly/1jd4f9c.

58 Tessa Morris-Suzuki, "Freedom of Hate Speech; Abe Shinzo and Japan's Public Sphere," *The Asia-Pacific Journal* 11, no. 1 (2013): 1-5, http://bit.ly/1L90LvC.

59 Keiko Tanaka, "Japan's Citizen Media Meet at Mikawa Medifes 2014," *Global Voices*, May 4, 2014, http://bit.ly/1hsF0OP.

60 Roger Pulvers, "Danger lurks when self-restraint segues into media self-censorship," *The Japan Times,* January 10, 2010, http://bit.ly/1Nq7dUR.

61 Keiko Tanaka, "Online Journalist Barred from Japan's Diet Press Hall," *Global Voices,* October 12, 2012, http://bit.ly/1L1S9t1.

62 Reporters Without Borders, "Freelance Journalists Face Discrimination On Fukushima Plant Visit," May 23, 2012, http://bit.ly/1Rw6qAu.

closed in 2008. The U.S.-based *Huffington Post* digital media website launched a Japanese-language version in 2013.[63]

YouTube, Twitter, Facebook, and international blog-hosting services are freely available, as are popular domestic platforms like Niconico Dōga, a video-sharing site, and LINE, a Korea-based chat application that was launched in Japan in 2011.

Digital Activism

To date, much digital activism has been effective at the local rather than national level, including maps sharing public information about disaster relief,[64] or tracking racist graffiti in Tokyo.[65] During the coverage period, anti-hate speech advocates using the internet to draw attention to and combat online slurs saw progress in a number of initiatives. In early 2015, a group of Korean residents and Japanese supporters established the Antiracism Information Center, which has a website and a physical location in Tokyo, to counteract hate speech online.[66] In May 2015, the Japanese video streaming website Niconico Dōga reported that it "shut down the official channel of the anti-Korean activist group *Zaitokukai*, citing violations of [its] terms of service.[67] Politicians also responded. In September 2014, the Kunitachi city assembly "adopted a statement demanding the central government take legislative action to ban 'hate speech' rallies.[68] Separately, in December 2014, a Japanese internet activist and academic erected a whistleblower website to challenge the state secrets law.[69]

Violations of User Rights

During the 2014-15 coverage period, two important pieces of legislation passed into law that may have implications for digital freedom of expression. After passage in the Lower House, the state secrets law, which some fear could threaten free expression, underwent several refinements before coming into force in December 2014. However, these revisions failed to address criticisms about the potential penalties attached to revealing information in the public interest. Separately, a law criminalizing revenge porn and other forms of online harassment passed in November 2014.

Legal Environment

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." [70] In general, individuals and media can exercise this in practice, though social and legal constraints exist.

The Act on the Protection of Specially Designated Secrets came into force in December 2014 after

63 Arianna Huffington, "Postcard From Japan: Talking Zen, Abenomics, Social Networking and the Constitution With Prime Minister Shinzo Abe," *Huffington Post,* May 9, 2013, http://huff.to/1MhvStk.

64 Keiko Tanaka, "Japan: OpenStreetMap Aggregates Typhoon Info," *Global Voices,* October 18, 2013, http://bit.ly/1jd6h9c; Keiko Tanaka, "Mapping Earthquake Reconstruction in Tohoku, Japan," *Global Voices*, October 7, 2013, http://bit.ly/1PjWKd0.

65 Keiko Tanaka, "Countering Hate Speech in Tokyo's Koreatown," *Global Voices*, March 6, 2014, http://bit.ly/1Rw5GLE.

66 Akira Nakano, "Antiracism website aids ethnic Korean victims of hate speech in Japan," *The Asahi Shimbun*, May 10, 2015.

67 "Video posting site shuts down anti-Korean Zaitokukai activists' channel," *The Japan Times*, May 20, 2015.

68 "Kunitachi city adopts statement to outlaw 'hate speech'," *The Asahi Shimbun*, September 24, 2014.

69 "Japanese activist challenges secrets law with whistleblower website," *Japan Today*, December 22, 2014.

70 The Constitution of Japan, November 3, 1946, http://bit.ly/1lLp7Tm.

passing in 2013, despite objections from the opposition, civil society, and protesters. The law gives a range of officials the discretion to indefinitely restrict public information pertaining to national security in any one of the categories of defense, foreign affairs, "prevention of designated harmful activities" (such as "counter-intelligence"), and prevention of terrorism.[71] Overseen by government officials rather than an independent body, it offers no protection for whistleblowers who reveal wrongdoing, leaving it open to misuse against Wikileaks-style whistleblowers and journalists.[72] For those people who handle such state-designated secrets, intentional leaks are punishable by up to 10 years' imprisonment, and unintentional leaks by up to 2 years. Individuals who knowingly receive such secrets from an administrative organ for the sake of the public interest risk up to 5 years for intentional disclosures and 1 year for disclosures via negligence.[73]

Refinements to the law during the coverage period outlined four main fields (defense, diplomacy, anti-espionage, and antiterrorism measures) in which 55 categories of state secrets can be applied.[74] Responding to criticism,[75] the government solicited public comments for a period of 30 days in July and August 2014.[76] After receiving more than 20,000 public comments,[77] draft revisions were tabled. Yet even these drew concerns, particularly in terms of how the law would actually work in practice.[78] In October 2014, protests continued throughout the country prior to the bill's coming into force in December.

Other laws include potentially disproportionate penalties for online activity, including a 2012 legal revision targeting copyright violators—including any internet user downloading content they know has been illegally copied, as opposed to just those engaged in piracy for commercial gain.[79] 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 JPY 10 million (US$102,000), the version in effect since October 1, 2012 added two years in jail or fines up to JPY two million (US$20,500) for downloading a single pirated file.[80] The Japanese Bar Association said that downloading, as an essentially insignificant personal act, should be regulated by civil instead of criminal laws.[81]

A 2013 revision of the Public Offices Election Act undid long-standing restrictions on use of the internet for election campaigns. Limits remain 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.[82] While these provisions were contested and revisions are still planned,[83] news reports said politicians vio-

71 Prime Minister of Japan, "Overview of the Act on the Protection of Specially Designated Secrets (SDS)," 2013, http://bit.ly/1OobNSj.

72 "Weak state secrets oversight," *The Japan Times*, July 28, 2014, http://bit.ly/1Mgu5QZ.

73 Cabinet Secretariat, "Overview of the Act on SDS Protection: 5. Penalty and Others," Preparatory Office for Enforcement of the Act on the Protection of Specially Designated Secrets," http://www.kantei.go.jp/jp/topics/2013/headline/houritu_gaiyou_e.pdf#page=6&zoom=auto,-8,62.

74 "State secrets to be refined into 55 fields," *The Japan News (Yomiuri Shimbun)*, July 18, 2014.

75 "Government revising guidelines on state secrets amid flurry of criticism," *The Japan Times*, September 20, 2014, http://bit.ly/1VHejsH.

76 "Government revising guidelines on state secrets amid flurry of criticism."

77 "Gov't sets guidelines on state secrets as concerns remain over arbitrary designation," *Mainichi Shimbun*, October 15, 2014.

78 "Kansai's fears of new law no state secret," *Japan Times*, October 26, 2014.

79 Daniel Feit, "Japan Passes Jail-for-Downloaders Anti-Piracy Law," *Wired,* June 21, 2012, http://wrd.cm/1hsGKaV.

80 Maira Sutton, "Japan's Copyright Problems: National Policies, ACTA, and TPP in the Horizon," *Deeplinks Blog,* Electronic Frontier Foundation, August 21, 2012, https://www.eff.org/deeplinks/2012/08/copyright-japan.

81 "Japan Introduces Piracy Penalties for Illegal Downloads," BBC, September 30, 2012, http://bbc.in/1g7S3gn.

82 "Editorial: Internet election campaigns can change Japan's politics," *Asahi Shimbun,* April 20, 2013, http://bit.ly/1cOFsVZ.

83 Ida Torres, "Japan's Internet election campaigning ban one step closer to being lifted," *Japan Daily Press,* April 4, 2013,

lating these restrictions face a potential JPY 300,000 (US$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 email could be fined JPY 500,000 yen (US$5,100) or jailed for two years, which would also deprive them of political rights.[84]

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.[85] However, it does not define what constitutes obscenity, leading to concerns that it may infringe on artistic expression and LGBTI rights.[86]

In June 2014, a law passed punishing possession of images of child sexual abuse, with a possible penalty of one year imprisonment.[87] In January 2015, police raided Amazon Japan's head office and affiliated distribution center after complaints the website was facilitating the sale of illegal material depicting children.[88] The company said it was cooperating.

Heightened awareness of revenge porn and online harassment culminated in the ruling Liberal Democratic Party (LDP) passing a bill criminalizing revenge porn in November 2014. The law stipulates that "offenders who distribute such images could face up to three years in prison or a fine of up to JPY 500,000 yen ($5,100), with third-party distribution also leading to up to one year in prison or a fine of JPY 300,000 yen ($3,060).[89]

In August 2014 the UN Committee on the Elimination of Racial Discrimination advised the Japanese government to enact laws to address hate speech, including statements made on the internet and offline.[90] A national bill has yet to be drafted.

Prosecutions and Detentions for Online Activities

While no citizens faced politically-motivated arrest or prosecution for content they have published online, in May 2015, police arrested a 43-year-old Tokyo resident for posting an online threat in the 2channel bulletin board against Princess Kako, a member of the Japanese royal family.[91] In February 2015, news reports said 40 people were arrested for illegally uploading copyrighted material.[92] No disproportionate sentences were reported.

Surveillance, Privacy, and Anonymity

Japan's Supreme Court protects privacy through its interpretation of Article 13 of the constitution,

http://bit.ly/1R1hVPk.

84 Ayako Mie, "Election campaigning takes to Net," *The Japan Times, April 11, 2013, http://bit.ly/1GyqxaQ;* "Japanese parliament permit use of Internet campaigning during elections," *TJC Global* (blog), April 20, 2013, http://bit.ly/1LBPvNV.

85 James R. Alexander, "Obscenity, Pornography, and the Law in Japan: Reconsidering Oshima's *In the Realm of the Senses*," *Asian-Pacific Law and Policy Journal* 4, no.1 (2003): 148-168, http://bit.ly/1OodGhM; Keiho [Penal Code] Act No. 45 of April 24, 1907, [in Japanese] http://bit.ly/1JVbWGD.

86 Keiko Tanaka, "Japan's Porn Law is Strangling Artists," February 18, 2013, http://bit.ly/1VHbkLA.

87 "Japan bans child pornography possession," *BBC*, June 18, 2014, http://bbc.in/1qc3U5j.

88 "Police search Amazon over online sale of child porn," *Asahi Shimbun*, January 24, 2015.

89 "Release of explicit images without consent to be criminalized," *Japan Times*, November 18, 2014.

90 "U.N. panel urges Japan to regulate hate speech by law," *Japan Times*, August 30, 2014.

91 "Man arrested for threatening Princess Kako online," *Japan Today*, May 22, 2015.

92 "40 People Arrested For Illegal Uploads Of Anime And Dramas This Past Week," *Arama Japan*, http://bit.ly/1R1iNDK.

which provides for the right to life and liberty.[93] "Secrecy of communication" is also protected under telecommunications laws,[94] though some digital activities require registration. Major mobile carriers require customers to present identification documents in order to subscribe, while prepaid SIM cards are not widely available. Internet cafe 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.

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.[95] A law enacted in 2003 and revised in 2008 prohibits electronic communications encouraging sexual activity with minors.[96] Under the law, all online dating services must register with the 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.[97] 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 past,[98] lawmakers were seeking to expand it in December 2012.[99] Critics say the law does not prevent the systematic storage of intercepted communications or protect innocent parties.[100] Security agents and the military have been accused of implementing surveillance in cases involving national security.[101]

A law to protect personal information dating from 2003 protects individuals' data collected electronically by private and public sector organizations, where the data involves more than 5,000 records.[102] Law enforcement requests for this data should be supported by a warrant.[103] In mid-2014, local news reported that 115 supermarkets and convenience stores in the Tokyo area had contracted with a Nagoya-based software firm to automatically record images of shoplifters and unreasonable customers to share in a network for other stores to blacklist.[104] While the businesses cited security measures,

93 Privacy International, "Chapter i: Legal Framework," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/i-legal-framework.

94 Ministry of Internal Affairs and Communications, Telecommunications Business Act, Act No. 86 of December 25, 1984, http://bit.ly/1ZhfM8n.

95 Carolina A. Klein, "Live Deaths Online: Internet Suicide and Lethality," *American Academy of Psychiatry and the Law* 40, no. 4 (December 2012): 530-536, http://www.jaapl.org/content/40/4/530.full.

96 Akira Saka, "Regulation for Online Dating in Japan,"(presentation Keio University, Japan, 2008) http://bit.ly/1GyrZtI.

97 Privacy International, "Chapter ii: Surveillance," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/ii-surveillance-policy.

98 In 1997, a court ordered the government to pay a senior member of the Japanese Communist Party 4 million yen [US$35,500] in damages for illegally wiretapping his residence in the 1980s. See, "Tokyo, Kanagawa Bow to Wiretap Ruling," *The Japan Times,* July 7, 1997, http://bit.ly/1P0TRhW.

99 Tsuyoshi Tamura, "Legal panel to discuss wiretapping for wider range of crimes," *Asahi Shimbun,* December 25, 2012, http://bit.ly/1L95TjI.

100 Privacy International, "Chapter ii: Surveillance."

101 Reuters, "Japan's Military Watched Citizens: Communist Party," *bdnews24*, June 6, 2007, http://bit.ly/1PjY3ss.

102 Business Software Alliance, "Country Report: Japan."

103 Privacy International, "Chapter iii: Privacy Issues," in Japan, December 12, 2006, https://www.privacyinternational.org/reports/japan/iii-privacy-issues.

104 "Stores sharing shoppers' faces," *The Japan Times*, April 12, 2014, http://bit.ly/1hsIYXV.

critics said sharing biometric data without consent conflicts with Japan's personal privacy law, Act on the Protection of Personal Information, No. 57 of 2003, which includes facial images within its definition of personal information. Amendments to the personal privacy law passed in September 2015, outside the coverage period of this report.

A "My Number" law proposed by the cabinet in 2012 passed the Diet on May 24, 2013.[105] Under this system each resident (including non-Japanese residents) will be assigned a unique ID number from October 2015.[106] Starting from January 2016, this number, which appears on a photo-ID card containing an electronic data chip, will be used for unified social-welfare services, including taxes, pensions, and healthcare.

The "My Number" system is the most recent in a series of attempts to nationally unify Japan's Basic Resident Registry procedures. The first was made in 2002 with the introduction of the Resident Basic Register Network System (known as RRNS or "Juki Net"), which was established to facilitate sharing information among local governments in the case of residents who move, register births and deaths, and apply for social services.[107] Even upon its introduction, the issue of a nationally available registry service was contested based on privacy issues, with some local municipalities choosing to opt out of the system (such as Tokyo's Suginami Ward and Yamatsuri town in Fukushima prefecture).[108] However, in response to a suit filed by 12 individuals in Aichi prefecture, the Supreme Court ruled in 2008 that Juki Net was constitutional and all citizens were subject to mandatory enrollment.[109]

Politicians and bureaucrats said personal identification numbers would streamline social benefits and maintain accuracy and fairness in the provision of government services,[110] as well as assist in identifying individuals in the case of natural disasters.[111] However, it remains unclear how the data would be stored in order to provide services offered through multiple levels of government.[112] The Japan Federation Bar Association in 2012 highlighted the system's possible privacy issues when the bill was first introduced.[113] In May 2013, the Japan Medical Association also contested the new system based on security issues involving medical records.[114] Others said its planned expansion into other government-related services, including potential use by the private sector, could also facilitate fraudulent use of personal data.[115]

Concerns about the implications of "My Number" for data privacy and security increased in 2014 with the arrest and subsequent trial of an engineer employed by a subsidiary data management company affiliated with the corporate group Benesse. He was charged with facilitating the country's largest personal data leak on record for the educational services company. Benesse "confirmed the leak of personal data of at least 7.6 million people [noting that]…the problem could ultimately affect

105 "EDITORIAL: ID number system should be a tool to build a fair society," *The Asahi Shimbun*, May 27, 2013, http://bit.ly/1hsJftU.

106 "'My number' is dangerous," *The Japan Times*, May 30, 2013, http://bit.ly/1VHiSTV.

107 Rebecca Bowe, "In Japan, National ID Proposal Spurs Privacy Concerns," *Deeplinks Blog*, Electronic Frontier Foundation, June 13, 2012, http://bit.ly/1OofXJQ.

108 "Juki Net constitutional, high court rules," *The Japan Times*, February 2, 2007, http://bit.ly/1hsJxkv."

109 Bowe, "In Japan, National ID Proposal Spurs Privacy Concerns."

110 "EDITORIAL: ID number system should be a tool to build a fair society," *The Asahi Shimbun*.

111 "Lower House passes 'my number' bill," *The Japan Times,* May 10, 2013, http://bit.ly/1L1We0n.

112 "'My number' is dangerous," *The Japan Times*.

113 Japanese Bar Association, "Statement Submitted to Parliament and the Cabinet Regarding the 'Social Security and Tax Number System' Bill," February 15, 2012, http://www.nichibenren.or.jp/activity/document/statement/year/2012/120215_6.html.

114 Bowe, "In Japan, National ID Proposal Spurs Privacy Concerns."

115 "'My number' is dangerous," *The Japan Times*.

more than 20 million."[116] A public opinion survey conducted by the Cabinet Office in January 2015 found that while only 28 percent of respondents were aware of the "My Number" system, nearly a third were concerned that "My Number" information could be used for unauthorized purposes.[117]

Intimidation and Violence

No physical violence has been reported against bloggers or internet users in relation to their online activity.

Technical Attacks

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,[118] they are not known to have been used to systematically target individuals or civil society groups. However, 1.25 million citizens were affected when hackers released personal information obtained by illegally accessing Japan's pension system using an email virus in mid-2015.[119]

Japanese law enforcement agencies are expanding their cybercrime capacity to respond to foreign cyberattacks and domestic data leaks. The National Policy Agency announced a new Cyberattack division in January 2015**.** In 2013, the Kanagawa and Osaka police departments established separate divisions for addressing cybercrime,[120] adding to police departments in Tokyo and 12 other prefectures.[121] Later that year, the Abe administration added the legislative position of "Chief Information Officer" to the national-level cabinet,[122] and the Information Security Policy Council within the National Information Security Center released a "Cybersecurity Strategy,"[123] and an "International Strategy on Cybersecurity Cooperation."[124]

The central government has become increasingly aware that there is a shortage of data specialists and data engineers within the government ranks. In January 2015, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was launched, "serv[ing] as a base of operations for [...] cybersecurity."[125] In the first few months of operations, the NISC received applications from private-sector programmers with an eye to recruiting up to 10 employees (to be employed "as

116 "1,789 file Y100 mil damages suit against Benesse over data leak," *Japan Today*.

117 "Editorial: Gov't must explain purpose of 'My Number' identification system," *The Mainichi,* March 31, 2015, http://bit.ly/1FUXUd4.

118 "Over 1,000 targeted cyber-attacks hit Japanese entities in 2012," *The Japan Times,* March 1, 2013, http://bit.ly/1LBUFtq.

119 William Mallard and Linda Sieg, "Japan pension system hacked, 1.25 million cases of personal data leaked," eds. Robert Birsel and Clarence Fernandez, *Reuters,* June 1, 2015, http://reut.rs/1QkFnWy.

120 Ida Torres, "Japanese police beef up in the fight against cybercrime," *Japan Daily Press*, June 11, 2013, http://bit.ly/1MgyKCj.

121 John Hofilena, "Japan's National Police Authority launches cyber-defense center," *Japan Daily Press*, May 17, 2013, http://bit.ly/1LoI0DP.

122 Prime Minister of Japan and His Cabinet, "Press Conference by the Chief Cabinet Secretary (Excerpt)," June 4, 2013, http://bit.ly/1LkeqDA.

123 Information Security Policy Council, *Cybersecurity Strategy,* June 10, 2013, 19-21, http://bit.ly/1cPLENI.

124 Information Security Policy Council, *International Strategy on Cybersecurity Cooperation,* October 2, 2013, http://bit.ly/1P0WXTk.

125 Andres Oliver, "Japan government to recruit 'white hat' hackers for landmark cybersecurity initiative," *Rocket News 24*, March 10, 2015, http://bit.ly/1AcSv7C.

government employees for up to five years"), as well as a staff of 100 people.[126] Also in the early months of 2015, the government aimed at recruiting such workers through sponsored events such as "hackathons." A "cybersecurity competition" was held in early February 2014 (Security Contest 2014, or SECCON), drawing a total of "4,186 participants of 58 different nationalities" with the final rounds being held among "90 participants in 24 teams from seven nations and regions."[127] Despite the increased focus by the central government, it remains to be seen if recruitment measures will be continued on a permanent basis (which would make them subject to the age restrictions and the examination system for all national, prefectural, and local civil servants) or if national, prefectural, and local governments will turn to private-sector information-technology companies as suppliers of technical staff on an outsourced contract basis.

126 Oliver, "Japan government to recruit 'white hat' hackers for landmark cybersecurity initiative."

127 "Tokyo cybersecurity contest draws hackers from around the world," *The Japan Times*, February 7, 2015, http://bit.ly/1NqebJA.