GERMANY

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	5	3
Violations of User Rights (0-40)	7	8
Total (0-100)	**16**	**15**

* 0=most free, 100=least free

POPULATION: 82 million
INTERNET PENETRATION 2011: 83 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Germany has a high level of internet and mobile penetration. Media and internet freedom are generally well-respected but have been challenged in recent years by legislative initiatives on blocking of harmful content, as well as surveillance measures by secret services and the police. Nevertheless, 2011 and early 2012 were characterized by a remarkable mainstreaming of internet issues. Topics such as copyright protection, net activism, access blocking, and online surveillance experienced significant attention in federal and state parliaments, major newspapers, and on television.

The growing political relevance of internet-related topics is partly due to an active, articulate, and well-networked civil society, which successfully framed issues such as access blocking in terms of threats to freedom of expression or as incompetence of established political actors in internet regulation. Consequently, in December 2011 the Federal Parliament repealed the Access Restriction Act, which called for blocking of child pornography websites, and instead, most political parties now support the system of take down notices and criminal prosecutions of those who post such content. Internet freedom was also a subject of several important court judgments including a decision to protect as free speech the posting of links that may lead to copyright infringing websites.

Nevertheless, several recent measures, taken by secret services and police in the context of surveillance, violated users' rights and potentially overstepped the existing laws. In October 2011, it became publicly known that the police in several German states used a Trojan-like piece of software in order to spy on criminal suspects. Also, the police systematically used

traffic data obtained by means of radio cell queries to investigate a series of car burnings in Berlin and demonstrations in Dresden

OBSTACLES TO ACCESS

Germany has a very well-developed information and communication technology (ICT) infrastructure, and 73 percent of the population has internet access at home, representing an increase by 6 percentage points between 2010 and 2011.[1] According to the International Telecommunication Union (ITU), overall internet penetration in Germany stood at 83 percent in 2011,[2] and the vast majority of users (86 percent) access the internet through DSL-technology. Alternative connections such as cable and LTE are slowly gaining market share (rising from 10 percent in 2009 to 13 percent in 2011), while 16 percent of the population still relies on dial-up connections.[3] A recent survey by Eurostat shows broadband adoption by Germany households at 78 percent, 10 percentage points above the European Union (EU) average.[4] With regard to high-speed broadband connections above 50 Mbps, there is currently a striking gap between supply and demand. While more than 40 percent of German households have access to high-speed internet connections thanks to well-developed cable networks, the subscriber rate is only 2 percent. Current broadband internet flat rates range from 15€ to 40€ per month (US$20 to $55) depending on the bandwidth of connection.

Most schools in Germany provide computers and internet access to their students mainly in dedicated computer rooms. Only 25 percent of German schools have classrooms equipped with computers.[5] According to an international survey by the World Economic Forum,

[1] Birgit van Eimeren and Beate Frees, *Ergebnisse der ARD/ZDF-Onlinestudie 2011* [Findings of the ARD/ZDF Online Survey 2011], 2011, p. 335, http://www.ard-zdf-onlinestudie.de/ (accessed March 20, 2012).
[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[3] Bundesministerium für Wirtschaft und Technologie [BMWi, Federal Ministry of Economics and Technology], *Breitbandatlas 2011* [Broadband Atlas 2011], 2011a, p. 5, http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-mitte-2011-teil-1,property=pdf,bereich=bba,sprache=de,rwb=true.pdf; Bundesnetzagentur [Federal Network Agency], *Tätigkeitsbericht 2010/2011 Telekommunikation* [Report 2010/2011 Telecommunications], 2011, p. 34, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile; Initiative D21, (N)Onliner Atlas 2011, 2011, p. 61, http://www.initiative21.de/wp-content/uploads/2011/07/NOnliner2011.pdf.
[4] BITKOM, "Breitband-Anschlüsse: Deutschland in der Spitzengruppe" [Broadband connections: Germany in the leading group], Press Release, January 31, 2012, http://www.bitkom.org/de/markt_statistik/64042_71099.aspx. The Federal Network Agency provides different numbers based on provider subscription data it reports 27 million households with a broadband connection (Bundesnetzagentur, 2011, p. 34). For the sake of comparison, the data provided by Eurostat have been chosen.
[5] Initiative D21, "Bildungsstudie: Digitale Medien in der Schule" [Digital Media in Schools], 2011, p. 8-9, http://www.initiative21.de/wp-content/uploads/2011/05/NOA_Bildungsstudie_140211.pdf (accessed 20 March 2012).

Germany ranks tenth among the 15 most developed ICT countries in terms of internet access in schools.[6] Meanwhile, the difference between urban and rural internet access is decreasing with rural areas having higher growth rates. For example, Berlin and Bremen have an 80 percent broadband penetration, while rural Mecklenburg-Vorpommern has 67 percent.[7]

While the gender difference in younger demographics of internet users is disappearing, it persists in the population above 50 and especially among the elderly over 70.[8] Men also significantly outnumber women in the adoption of mobile internet access (26 percent vs. 13 percent). Levels of formal educational remain a crucial factor influencing the use of the internet, as 90 percent of people with higher education access the internet regularly compared to 60 percent of Germans with basic education. However, these gaps are beginning to close as internet penetration increases. In contrast, income-related differences in internet use have persisted: only 53 percent of households with a monthly income below €1,000 (US$1,280) access the internet from home compared to 92 percent of households with an income higher than €3,000 (US$3,835).[9]

Mobile phone penetration in Germany is almost universal, with a penetration rate of over 132 percent at the end of 2011.[10] Only Finland, Italy and Great Britain have higher penetration rates.[11] However, the adoption of mobile internet is below the EU average, with only 28 percent of Germans accessing the internet by phone (compared to 34 percent in the EU).[12] Germany's 3G coverage of 89 percent is also slightly below the EU average.[13]

The telecommunications sector was privatized in the 1990s with the aim of fostering competition. Over the past decade, market consolidation has led to a competitive environment dominated by large companies both in fixed-line as well as mobile internet access; consequently, several smaller internet service providers (ISPs) have been forced out of business. The incumbent Deutsche Telekom's share of the broadband market is 46

[6] Bundesministerium für Wirtschaft und Technologie [BMWi, Federal Ministry of Economics and Technology], *Monitoring-Report Deutschland Digital 2011*, 2011b, p. 75, http://www.bmwi.de/Dateien/BMWi/PDF/IT-Gipfel/ikt-monitoring,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.
[7] BMWi, 2011a, Breitband-Atlas 2011.
[8] Eimeren and Frees 2011, p. 337; Initiative D21, 2011, (N)Onliner 2011, p. 42.
[9] Initiative D21, 2011, (N)Onliner 2011, p. 16.
[10] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] Bundesnetzagentur, 2011, p. 50; BMWi 2011b, Monitoring, p. 101.
[12] BMWi, 2011b, Monitoring, p. 119.
[13] European Commission, "3G coverage (as a % of total population)," Digital Agenda Scoreboard Survey 2011, accessed March 20, 2012, http://cl.ly/FL2U.

percent. Other relevant ISPs are 1&1 (United Internet), Arcor (Vodafone), Telefónica, and Kabel Deutschland.[14]

There are four general carriers for mobile internet access: market leader Vodafone (33 percent), incumbent T-Mobile (31 percent), E-Plus (19.8 percent), and Telefonica (16.2 percent). The latter two are more recent market entrants with higher growth rates that have resulted in a redistribution of market shares.[15] In effect, the mobile market is seen as one of the most competitive in the EU,[16] though competition in downstream markets of mobile services such as Voice over Internet Protocol (VoIP) or instant messaging is limited, since all German mobile providers contractually prohibit or limit these services. Nevertheless, these prohibitions have yet to be enforced systematically by the carriers.[17]

Management of network traffic and bandwidth availability is very common.[18] The online platform RespectMyNet.eu,[19] initiated in 2011 by La Quadrature Du Net and Bits of Freedom to collect and publish information on violations of net neutrality in Europe, shows that German users most frequently report the (temporary) throttling of YouTube data, the blocking of peer-to-peer (P2P) websites, and the contractual blocking of internet protocol (IP) telephony servers for mobile internet. Although practically all ISPs support net neutrality in theory, they nonetheless include in their general terms and conditions constraints on internet access. Typical services subject to exclusion or restrictions are tethering (the use of smart phones as a router for providing internet accessing to other devices), VoIP, and limitations of the monthly data volume included in flat rates.

Internet access, both broadband and mobile, is regulated by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (Bundesnetzagentur, or BNetzA) operating under the supervision of the Federal Ministry of Economics and Technology. The president and vice president of the agency are appointed for five-year terms by the federal German government following recommendations from an Advisory Council consisting of 16 members of the lower house of parliament and 16 representatives of the upper house. The German Monopoly Commission and the European Commission (EC) have both criticized

[14] European Commission, "New entrants' share in fixed broadband lines," Digital Agenda Scoreboard 2011, accessed March 20, 2012, http://cl.ly/FK1q.
[15] Bundesnetzagentur, 2011, p. 51.
[16] EU Digital Agenda Scoreboard 2011. Electronic Communications Market Indicators, p.10, accessed March 20, 2012. Cf. also the study by Haucaup et al. documenting a fairly competitive market: Haucap/Heimeshoff/Stühmeier, 2010, Wettbewerb im Deutschen Mobilfunkmarkt: Ordnungspolitische Perspektiven Nr. 4.
[17] Call Magazin, "Brüssel will das Blocken von VoIP-Diensten stoppen," April 21, 2011, http://www.call-magazin.de/handy-mobilfunk/handy-mobilfunk-nachrichten/bruessel-will-das-blocken-von-voip-diensten-stoppen_29988.html.
[18] See the report of the Parliamentary Inquiry Commission Internet and Digital Society on net neutrality: p. 12, www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Netzneutralitaet_Zwischenbericht_1708536.pdf.
[19] Respect My Net website: http://respectmynet.eu/.

this highly political setting and the concentration of important regulatory decisions in the presidential chamber of the Federal Network Agency.[20] The appointment of President Jochen Homann, the former state secretary in the supervising federal ministry who took over the post from Matthias Kurth after he was surprisingly dismissed in February 2012, seems to affirm the concern over a lack of independence. Similarly, the European Court of Justice (ECJ) and the EC noted that the regulation of data protection and privacy by agencies under state supervision does not comply with the EU Data Protection Directive 95/46/EC.[21]

In addition to such institutional concerns, regulatory decisions by the BNetzA have been criticized for providing a competitive advantage to Deutsche Telekom, the former state-owned monopoly.[22] The most recent example of preferential treatment has been the setting of the price the incumbent is allowed to charge competitors for the "last mile,"[23] yielding one of the highest prices in Europe.[24] The industry associations Eco and BITKOM represent the political and economic interests of ISPs and regularly participate in debates concerning provider liability, copyright enforcement, and access blocking.

LIMITS ON CONTENT

While the blocking of websites rarely takes place in Germany, court orders mandating the deletion of websites have been a common occurrence. Due to substantial criticism by activists and NGOs that provoked an intense political debate, the 2010 law on blocking websites containing child pornography, the Access Restriction Act (Zugangserschwerungsgesetz),[25] never came into effect and was finally repealed by the

[20] Monopolkommission [Monopoly Commission], *Telekommunication 2009: Klaren Wettbewerbskurs halten* (Berlin: Monopolkommission, 2009), 75, http://www.monopolkommission.de/sg_56/s56_volltext.pdf [in German]; European Commission, *Progress Report on the Single European Electronic Communications Market, 15th Report* {COM(2010) 253}, 196, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/15report_part1.pdf.

[21] European Commission, "Data Protection: European Commission requests Germany to ensure independence of data supervisory authority," press release, Brussels, April 6, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/407&format=HTML&aged=0&language=EN&guiLanguage=en.

[22] European Commission, *Progress Report*, 196.

[23] The final leg of delivering connectivity from a communications provider to a customer, see http://en.wikipedia.org/wiki/Last_mile.

[24] For an overview on European prices, cf. the international tariff comparison by the BNetzA, accessed March 20, 2012, http://cl.ly/FW13. For the criticism of the competitors cf. "Telekom muss Miete für die letzte Meile kaum senken," golem.de, March 31, 2011, http://www.golem.de/1103/82473.html.

[25] Law on the reduction of access to child pornography in communication networks (Access Impediment law), February 17, 2010, http://beck-online.beck.de/default.aspx?typ=reference&y=100&g=ZugErschwG.

German parliament in December 2011.[26] The law would have required ISPs to block access to pages containing child pornography and authorized the Federal Criminal Office (BKA) to maintain continuously updated lists of sites to be blocked. All parliamentary parties have now agreed on the position put forward by the Working Group Against Internet Blocking and Censorship (AK Zensur)[27] supporting take down notices and prosecution rather than blocking as an appropriate remedy. Furthermore, attempts by the district council Düsseldorf, North Rhine-Westphalia, to block illegal gambling sites were rejected by various administrative courts.[28]

In response to an initiative by the European Commission on introducing access blocking at the EU level, German diplomats under the auspices of the German Department of Justice joined NGOs and members of the European Parliament in vetoing the proposed directive. In effect, the European Parliament and the European Commission agreed on a considerably weakened directive that no longer includes mandatory EU-wide blocking but rather stipulates that EU member states focus on the removal of webpages containing actionable content (such as child pornography) in and outside their territory.[29]

Evidence suggests that ISPs across Europe regularly use deep packet inspection for the purposes of traffic management but also to throttle peer-to-peer traffic.[30] In Germany, there is a clear lack of transparency regarding the scope of traffic management, in general, and the use of deep packet inspection, in particular, since ISPs are not required to make such information public.

There is no censorship prior to publication of internet content. However, figures released by the Google Transparency Report concerning requests by public authorities for post-

[26] EDRI, "German web blocking law repealed," EDRi-gram Newsletter, No. 9.24, December 14, 2011, http://www.edri.org/edrigram/number9.24/german-internet-blocking-law-repealed.

[27] Ak-Zensur website: http://ak-zensur.de/.

[28] Thomas Stadler, "Auch das VG Köln spricht sich gegen Netzsperren bei Glücksspielen aus" [Also, the Cologne Administrative Court is opposed to Internet blocking in games], Internet-Law (blog), January 12, 2012, http://www.internet-law.de/2012/01/auch-das-vg-koln-spricht-sich-gegen-netzsperren-bei-gluecksspielen-aus.html.

[29] Directive 2011/92/EU of the European Parliament and of the Council of December 13, 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, accessed March 20, 2012, http://eurlex.europa.eu/JOHtml.do?uri=OJ:L:2011:335:SOM:EN:HTML. For more information on the development of this directive, cf. "Provisional conclusion of negotiations on blocking," European Digital Rights Initiative (EDRi), accessed March 20, 2012, http://www.edri.org/blocking_negotiations, and the procedure file of the European Parliament, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?id=584949.

[30] "BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely," Body of European Regulators for Electronic Communications, press release, 2012, http://www.erg.eu.int/doc/2012/TMI_press_release.pdf. See also the preliminary report on net neutrality by the multi-stakeholder Commission of Inquiry (Enquete Kommission) on the Internet and Digital Society, set up by the German Federal Parliament in 2010: p. 12, http://www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Netzneutralitaet_Zwischenbericht_1708536.pdf .

publication content removal indicate that this strategy is used extensively. During the first six months of 2011, Germany ranked second behind Brazil among 62 listed countries with 125 government requests for the removal of 2,405 items.[31] In the last six months of 2011, Germany ranked third behind Brazil and the United States with 103 government requests to remove 1,722 items.[32] The most common reasons for court order requests were defamation, privacy, and security matters.

The protection of minors constitutes another important legal framework for the regulation of content. Youth protection on the internet is principally addressed by states through the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting (JMStV), which bans content similar to that outlawed by the criminal code such as the glorification of violence and sedition.[33] A controversial provision of the JMStV reflecting the regulation of broadcasting media mandates that adult-only content on the internet, including adult pornography, must be made available in a way that verifies the age of the user. Compliance with the interstate agreement is overseen by the Commission for Youth Protection Relating to Media. Importantly, the JMStV opens up the prospect of content being blocked if other actions against offenders fail and if the blocking of content is expected to be effective. Owners of offending websites residing outside of Germany are put on blacklists that are made available for privately-developed filtering software. Members of the self-regulatory body, Voluntary Self-control for Multimedia Service Providers (FSM), have committed to removing blacklisted websites from their search results.

In late 2010, the JMStV's planned amendment to introduce age rating for online content failed due to both procedural issues, particularly the lack of public consultation, and substantive issues. According to critics, the amendment did not sufficiently take into account the categorical differences between content made available by broadcasting media and the distributed mode of content production on the internet.

Although access providers are not responsible for the content they transmit, there is a certain tension between the underlying principles of liability privilege and that of secondary

[31] Google complied fully or partially with 86 percent of these requests. Google, "Germany," Google Transparency Report, January to June 2011, accessed August 2, 20122http://www.google.com/transparencyreport/removals/government/countries/?p=2011-06.

[32] Google complied fully or partially with 77 percent of these requests. Google, "Germany," Google Transparency Report, July to December 2011, accessed August 2, 20122, http://www.google.com/transparencyreport/removals/government/DE/?p=2011-12.

[33] Cf. the respective paragraphs 130 and 131 in the Crimical Code: http://dejure.org/gesetze/StGB/130.html; http://dejure.org/gesetze/StGB/131.html.

liability (breach of duty of care).[34] The Telemedia Act §8, based on Articles 12 to 14 of the European E-Commerce Directive, explicitly states that access providers are not legally responsible for the content they transmit over the internet unless they violate reasonable audit requirements or collaborate with users in unlawful behavior. Recent court rulings both on the national and the European level have confirmed the liability privilege for information intermediaries following several years of contradictory rulings. The liability privilege also applies to host providers who are not required to monitor content or install filtering devices. As the European Court of Justice ruled in the 2011 case "Scarlet Extended," "a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes fundamental rights."[35]

Another important ruling refers to liability for URLs. In the 2011 "AnyDVD" case, the German Federal Constitutional Court confirmed a lower court's decision that URLs belonging to copyright infringing websites are protected by freedom of expression and freedom of opinion.[36] Likewise, host providers are not liable for blog entries; they just have to act upon objections.[37] An important exception concerns wireless networks. In 2010, the German Federal High Court sentenced the private owner of a wireless router on the grounds that his or her open network allowed its use for illegal activities.[38] Because of the adverse effects of this judgment on the operators of open networks, the Berlin state legislature is planning to modify the secondary liability in question.[39]

The principle of proportionality has constitutional status in Germany to which public authorities must comply. There is no specific supervisory body in place to oversee the implementation of this principle. Yet, the interplay between the Ministry of Justice, national data protection officer, association of internet service providers (Eco), and internet community effectively hold the bodies involved to account.

[34] Liability privilege means that information intermediaries on the internet such as ISPs are not responsible for the content their customers transmit. Secondary or indirect liability applies when intermediaries contribute to or facilitate wrongdoings of their customers.

[35] Court of Justice of the European Union, PRESS RELEASE No 37/11, Luxumbourg, April 14, 2011, http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf.

[36] "German Constitutional Court confirms BGH's 'AnyDVD' copyright decision," The IPKate (blog), February 21, 2012, http://ipkitten.blogspot.de/2012/02/german-constitutional-court-confirms.html. For the concrete reasons given for the judgment, cf. the court's ruling: http://www.bundesverfassungsgericht.de/entscheidungen/rk20111215_1bvr124811.

[37] Cf. the opinion of the court: http://www.telemedicus.info/urteile/Internetrecht/1317-BGH-Az-VI-ZR-9310-Pruefpflichten-fuer-Hostprovider-Blogspot.html.

[38] Christopher Burgess, "Three Good Reasons to Lock Down Your Wireless Network," The Huffington Post (blog), June 8, 2010, http://www.huffingtonpost.com/christopher-burgess/three-good-reasons-to-loc_b_599945.html.

[39] "Berliner Initiative für offene WLANs" [Initiative for free WLAN in Berlin], heise.de, April 7th 2012, http://www.heise.de/newsticker/meldung/Berliner-Initiative-fuer-offene-WLANs-1517403.html.

Court proceedings are generally public, and there are no so-called gag orders that would restrict media coverage of ongoing law suits. While there is no comprehensive list of all content blocking or deletion orders, there is general media coverage of such measures. One important exception in reporting concerns the index of the Commission for the Protection of Minors in the Media (KJM) and the Federal Review Board for Media Harmful to Young People (BpJM), which are kept secret.

There is no systematic self-censorship in the German press; however, there are more or less unspoken rules codified in the publishing principles of the German press.[40] The code, which has the status of a voluntary commitment, specifies the ethical principles of journalism and seeks to strike a balance between the public interest and the protection of personal rights and privacy. Since 2009, these principles have applied to online journalism. The penalty code and JMStV prohibit content in a well-defined manner (e.g. child pornography, racial hatred, and the glorification of violence). The JMStV also regulates adult content that is potentially harmful to minors, stipulating that content unsuitable for certain age groups must be protected to prevent access by children or young individuals (see discussion on deletion of content).

In line with the European Commission's regulatory approach toward net neutrality, the German Federal Network Agency principally supports net neutrality but rejects its legal codification. At the same time, the national regulator has shown sympathy for the ISPs' practice of traffic management. The regulator is also open to new business models based on price discrimination and differentiated classes of service as long as ISPs are transparent about their policies and give customers a choice.[41] Yet, the latest amendment of the Law on Telecommunications (Telekommunikationsgesetz, TKG) adopted in December 2011 authorizes the government to define basic requirements for non-discriminatory data transfer and minimum quality of service standards in order to prevent a deterioration of internet services.[42]

The use of proxy servers is common in Germany but for the purpose of circumventing copyright provisions than to avoid censorship. There are no figures available about the extent of use.

[40] Cf. the codex of the German Press Council: http://www.presserat.info/uploads/media/Novellierter_Kodex_03.pdf.
[41] See the minutes of the Expert Meeting on net neutrality of the Parliamentary Inquiry Commission, October 8th, 2010, http://www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Gespraechsprotokoll_-_6_Sitzung_BNetzA_2010-11-08.pdf.
[42] See the report of the parliamentary board of economy and technology, October 26th, 2011: http://dipbt.bundestag.de/dip21/btd/17/075/1707521.pdf.

Germany is home to a vibrant internet community and blogosphere with growing political influence on public and private regulatory action. Policies affecting internet regulation, data protection, or surveillance are enjoying increasing public attention and media coverage. The disproportionate number of young males in the internet community is striking, however. The recent success of the Pirate Party (with 8.9 percent of the vote) and the Saarland (with 7.4 percent)—parties that are known for their strong positions in favor of the free sharing of knowledge and substantial reforms in copyright law—in state elections in Berlin confirms both the growing popularity of internet-related topics and the predominantly male composition of the internet community.

The multi-stakeholder Commission of Inquiry (Enquete Kommission) on the Internet and Digital Society, set up by the German Federal Parliament in 2010, has significantly contributed to the mainstreaming of internet issues.[43] All political parties by now have internet experts and feel the need to express and justify opinions on internet-related topics. Also, there are regular public interactions between politicians and the internet community on Twitter and blogs and at public events. An example of the growing discursive power of the internet community concerns the forced resignation of the defense minister in 2011 due to plagiarism exposed in detail on a dedicated website.[44] Another example involved the widespread demonstrations in roughly 60 German cities against the Anti-Counterfeiting Trade Agreement (ACTA) in early 2012, which led the minister of justice to make a political U-turn and put the signing of ACTA on hold.

VIOLATIONS OF USER RIGHTS

German Basic Law guarantees freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). These articles generally safeguard offline as well as online communication. In addition, a groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right warranting the "confidentiality and integrity of information technology systems" that is grounded in the general right of personality guaranteed by Article 2 of the Basic Law.[45]

[43] Cf. the website of the commission: http://www.bundestag.de/internetenquete/

[44] Cf. the website "GuttenPlag": http://de.guttenplag.wikia.com/wiki/GuttenPlag_Wiki.

[45] Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, Judgment of 27 February 2008, 1 BvR 370/07; 1 BvR 595/07, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html; See also, Press release no. 22/2008, http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html. For more background cf. W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822," (2009) 6:1 *SCRIPTed* 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

These rights were contested in the political aftermath of the September 2001 terrorist attacks in the United States (cf. the 2001 Act for Limiting the Secrecy of Letters, the Post, and Telecommunications).[46] However, after several cases concerning the infringement of journalists' rights, a Federal Constitutional Court ruling in February 2007 set a strong precedent for the protection of journalists' sources.[47] Following this ruling, the federal parliament issued in 2012 the Act on Strengthening Press Freedom (Gesetzes zur Stärkung der Pressefreiheit im Straf- und Strafprozessrecht, PrStG), which protects journalistic sources and establishes high barriers for searching and seizing journalists' properties.[48] In addition to the aforementioned rulings on the liability privilege of providers, these developments constitute a trend of strengthening media freedom in Germany. The rulings of the Federal Constitutional Court continue to promote freedom of expression in particular.

Online journalists are generally accorded the same rights and protections as journalists in print or broadcast. Although the functional boundary between journalists and bloggers is becoming blurry, the German federation of journalists maintains professional boundaries by handing out press cards only to full-time journalists. Similarly, the German Code of Criminal Procedure grants the right to refuse testimony solely to individuals who have "professionally" participated in the production or dissemination of journalistic materials."[49]

Incidents of confiscated video material covering demonstrations, for example, have led to a debate about extending the right to refuse testimony to a larger group. In August 2011, the Pirate Party filed a petition to the Federal Parliament asking to discard the term "professionally" in the relevant paragraph of the German Code of Criminal Procedure, but this issue has not gained a lot of attention.[50]

---

[46] This Act enables secret services to intercept, monitor, and record private communications, including the surveillance of journalists under specific conditions. It also restricts journalistic privileges such as the right to refuse to give evidence. "Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses" [Law on the restriction of correspondence, posts and telecommunications secrecy], Bundesministerium der Justiz, accessed March 20, 2012, http://www.gesetze-im-internet.de/g10_2001/index.html.

[47] Bundesverfassungsgericht [Federal Constitutional Court], "Cicero-Urteil," Decision 1 BvR 538/06, accessed March 20, 2012, http://www.bverfg.de/entscheidungen/rs20070227_1bvr053806.html. For the European context, see David Banisar, *Speaking of Terror: A Survey of the Effects of Counter-terrorism Legislation on Freedom of the Media in Europe* (Strasbourg: Council of Europe, 2008), accessed March 20, 2012, http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

[48] Cf. the press release of the Federal Ministry of Justice, accessed March 20, 2012: http://cl.ly/FVeK.

[49] Strafprossordnung (StPO) [Code of Criminal Procedure], Paragraph 53 (1) 5, accessed March 20, 2012, http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0198.

[50] File of the petition in the parliamentary epetition-system, accessed March 20, 2012, https://epetitionen.bundestag.de/index.php?action=petition;sa=details;petition=19350.

The German penal code (StGB) includes a paragraph on "incitement to hatred" (StGB §130), which penalizes calls for violent measures against minority groups and assaults on human dignity.[51] This provision is generally regarded as legitimate by the German population not least because it is mostly applied in the context of holocaust denials.

The anonymous use of email services, online platforms, wireless internet access points, and public telephone booths are legal. Although the federal minister of the interior and other members of the conservative parties have repeatedly expressed their disapproval of anonymity on the net,[52] this situation is not likely to change. With explicit references to the constitution, several courts have repeatedly affirmed the right to anonymity and its necessity for the exercise of the constitutional right to freedom of expression.[53] At the same time, the Telemedia Act (Telemediengesetz, TMG) and the Interstate Treaty on Broadcasting (Rundfunkstaatsvertrag, RFStV) mandate a legal notice that includes contact data for most websites and blogs.

Under Sections 112 and 113 of the Telecommunications Act, law enforcement agencies and prosecutors can obtain users' contractual data without a judge's order. For traffic and content data, however, judicial approval is required. The Federal Network Agency serves as the data collecting intermediary between telecommunications companies and law enforcement bodies. The agency reported six million requests from public authorities and 36 million queries directed to telecommunications service providers in 2010.[54] A small number of government entities are authorized, for narrowly circumscribed purposes, to request sensitive data under Section 113 of the Telecommunications Act (TKG). This data may include personal identity numbers (PINs), personal unblocking keys (PUKs), and passwords that allow access to devices or online services. Such inquiries may only be used to identify the person who generated a certain communication or connection at a certain point in time.[55]

---

[51] For an English translation of the German penal code see: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P130, accessed March 20, 2012.

[52] See for example, "Innenminister Friedrich will Blogger-Anonymität aufheben" [Federal Minister of Interior wants to abolish anonymity of bloggers], Tagesspiel online, August 7, 2011, http://www.tagesspiegel.de/politik/internet-innenminister-friedrich-will-blogger-anonymitaet-aufheben/4473060.html.

[53] Eg. Oberlandesgericht (OLG) Hamm [German Federal Court of Appeals Hamm], File I-3 U 196/10, August 3, 2011, http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html.

[54] The period from 2001 to 2010 shows a steady increase on both counts, from an initial 1.5 million requests from security authorities and 3.2 million queries by the Federal Network Agency in 2001, cf. Bundesnetzagentur, *Annual Report 2010*, 125, accessed March 20, 2012, http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/ReportsPublications/2011/AnnualReport2010pdf.pdf.

[55] This procedure was ruled as partly unconstitutional by the Federal Constitutional Court in January 2012. The legislative is asked to revise the paragraph until 30 June 2013. Federal Constitutional Court, Decision 1 BvR 1299/05, January 24, 2012, http://www.bundesverfassungsgericht.de/entscheidungen/rs20120124_1bvr129905.html.

Telecommunications interception by state authorities is regulated by the code of criminal procedure (StPO) and is understood as a serious interference with basic rights. It may only be employed for the prevention or prosecution of serious crimes for which specific evidence exists and when other less intrusive investigative methods are likely to fail. According to recent statistics published by the Federal Office of Justice, there were a total of 20,398 orders for telecommunications interception in 2010, of which 997 concerned internet communications. This is an increase of about 25 percent compared to 2008.[56] There were also a total of 12,576 orders asking for internet traffic data in 2010.[57]
Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figures. The competent Parliamentary Control Panel reported for 2011 a total of 37 million emails scanned, of which only 239 were considered relevant.[58]

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established a new fundamental right warranting the "confidentiality and integrity of information technology systems." The court held that preventive covert online searches are only permitted "if factual indications exist of a concrete danger" that threatens "the life, limb, and freedom of the individual" or "the basis or continued existence of the state or the basis of human existence." The court also established that any covert infiltration of information technology systems requires a court order and that statutes permitting such infiltrations must "contain precautions in order to protect the core area of private life."[59] Based on this Constitutional Court ruling, the Federal Parliament passed an act in 2009 authorizing the Federal Bureau of Criminal Investigation (BKA) to conduct covert online

[56] Bundesamt für Justiz [Federal Office for Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2010," July 29, 2011, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__TKUE__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2010.pdf [in German].
[57] Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2010," July 29, 2011, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__Verkehrsdaten__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2010.pdf [in German].
[58] Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 17/8639, February 10, 2012, http://dipbt.bundestag.de/dip21/btd/17/086/1708639.pdf. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G 10 Commission. The G 10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007. See also: http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html [in German].
[59] Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, Judgment of 27 February 2008, 1 BvR 370/07; 1 BvR 595/07, See also, http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html, accessed March 20, 2012. For more background cf. W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822," (2009) 6:1 *SCRIPTed* 106, accessed March 20, 2012, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

searches to prevent terrorist attacks on the basis of a warrant.[60] In addition to online searches, the act authorizes the BKA to employ methods of covert data collection including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect's computer that intercepts communications at their source.

In October 2011, the Chaos Communication Club (CCC), a German hacker organization, uncovered the use of a Trojan-like piece of software by the police for crime investigation purposes in several German states. The CCC's analysis of the software showed that the Trojan not only enables the police to (legally) eavesdrop on encrypted conversations but also allows for a far wider range of actions, which are illegal to deploy for both police and secret services. Among these encroachments include the searching of digital devices, logging of keystrokes, and even planting of "backdoors" that allow for the remote installment of additional software or insertion of false evidence. Five German states admitted the use of the "Bundestrojaner" (Federal Trojan) as such but denied the use of any illegal functions.[61]

Together with evidence that the police made use of radio cell queries in the context of the car burnings investigations in Berlin in late 2009 and demonstrations in Dresden in 2011 and 2012,[62] the proportionality of the surveillance measures must be questioned. However, the rulings of the Federal Constitutional Court form a strong counterweight to massive violations of user rights.

Following the EU Data Retention Directive, the 2007 Law on the Revision of Telecommunications Monitoring and other Covert Investigation Measures and the Implementation of Directive 2006/24/EC require ISPs and mobile phone companies to retain traffic data for six to seven months to facilitate criminal investigations. A constitutional complaint filed by nearly 35,000 individuals, including the justice minister herself, with the Federal Constitutional Court led to the repeal of the national data retention provisions in 2010.[63] A revision of the data retention law, as required by the European Commission, is still pending as of mid-2012. Under discussion is the option of a "quick freeze" procedure for traffic data which would allow for data to be stored only upon concrete preservation orders from law enforcement agencies. A legal opinion commissioned

[60] "Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten," http://www.gesetze-im-internet.de/bkag_1997/ (accessed March 20, 2012). Cf. Dirk Heckmann, "Anmerkungen zur Novellierung des BKA-Gesetzes: Sicherheit braucht (valide) Informationen," Internationales Magazin für Sicherheit nr. 1 (2009), http://www.ims-magazin.de/index.php?p=artikel&id=1255446180,1,gastautor [in German].
[61] Deutsche Welle, "Several German states admit to use of controversial spy software," October 11, 2011, http://www.dw.de/dw/article/0,,15449054,00.html.
[62] André Meister, "Massenhafte Funkzellenabfrage jetzt auch in Berlin: Was Vorratsdatenspeicherung wirklich bedeutet," Netzpolitik.org (blog), January 19, 2012, http://cl.ly/FjXb [in German].
[63] "Leitsätze zum Urteil des Ersten Senats vom2. März 2010" [Guidelines to the judgment of the First Senate of March 2, 2010], Bundesverfassungsgericht, accessed August 20, 2012, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

by the federal government expressed strong doubts about the compatibility of the data retention directive with the European Charter of Fundamental Rights.

As part of the data retention law, the government also revised the duty of identification, obliging ISPs to store contractual data of their customers. The obligatory identification concerns phone lines, SIM cards for mobile phones, and DSL connections. Email, WLAN services, and internet cafes are exempted from this obligation.

Building on the Safer Social Networking Principles for the EU,[64] the minister of interior suggested in 2011 that providers of social networks and search engines agree upon a code of conduct in order to support the protection of minors and that of consumers.[65] This initiative also follows a national code of conduct developed under the auspices of the organization for Voluntary Self-Monitoring of Multimedia Service Providers (FSM), which focuses on data protection for minors.[66]

As part of its cyber security strategy,[67] the federal government established in 2011 a cyber-defense center operating under the auspices of the Federal Office for Information Security, itself a subordinate body of the Federal Ministry of the Interior. In the face of an increasing number of cyberattacks, the German government has attached growing importance to the protection of "critical infrastructure."[68] Within the first months of its activity, the cyber-defense center apparently dealt with three to five cases of cybercrime a day.[69] Considering the potential impact of cybercrime and its conspicuous rise since 2009, the founding of a cyber-defense center is viewed as a useful if somewhat belated step.

[64] European Commission, "Safer Social Networking Principles for the EU," February 10, 2009, http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

[65] Innenministerium setzt auf Datenschutz-Selbstkontrolle von Facebook [German Government favors self-regulation by Facebook], heise.de, September 8, 2011. http://www.heise.de/newsticker/meldung/Innenministerium-setzt-auf-Datenschutz-Selbstkontrolle-von-Facebook-1339410.html.

[66] Cf. the code of conduct on the website of the FSM: http://fsm.de/de/Web_2_0.

[67] Cf. the policy paper on Cybersecurity of the Federal Ministry of Interior: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

[68] Cf. the press release of the Federal Ministry of Interior: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/06/cyber.html.

[69] "Täglich bis zu fünf Fälle für das Cyber-Abwehrzentrum" [Cyber-defense center handles five cases each day], FOCUS Online, June 8, 2011, http://www.focus.de/digital/computer/computer-taeglich-bis-zu-fuenf-faelle-fuer-das-cyber-abwehrzentrum_aid_635369.html.