GERMANY

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access	n/a	4
Limits on Content	n/a	5
Violations of User Rights	n/a	7
Total	**n/a**	**16**

POPULATION: 81.6 million
INTERNET PENETRATION: 72 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Telecommunications in Germany are an increasingly contested arena in which the state, civil society leaders, and powerful private companies including internet-service providers (ISPs) assert sometimes incompatible rights and interests. There is a great deal of legal uncertainty in two key areas of internet freedom: a data-retention law has been ruled unconstitutional, and controversy surrounding a new law for blocking internet content has prevented it from being applied to date. Furthermore, while the constitution contains strong privacy protections, and private companies that violate them have been held accountable, lawmakers have increasingly curbed privacy rights in certain contexts, particularly with respect to government-approved surveillance. On other issues, such as the liability of ISPs for content, conflicting court decisions have added to legal ambiguity.

OBSTACLES TO ACCESS

The infrastructure is well developed, with electricity and at least fixed-line telephony in all homes. Mobile-telephone access is ubiquitous. In 2009, there were a total of 108 million mobile subscriptions in Germany, compared with 82.7 million inhabitants.[1] In terms of internet access, 72 percent of the population over 14 years old were considered users in

[1] See BuddeComm, "Germany—Mobile Market: Statistics and Forecasts," https://www.budde.com.au/Research/Germany-Mobile-Market-Overview-Statistics-Forecasts.html, accessed September 2, 2010. For the development of mobile-phone access in Germany since 1990, see Bundesnetzagentur [Federal Network Agency], *Annual Report 2009* (Berlin: Bundesnetzagentur, 2010), 90, available at http://www.bundesnetzagentur.de/cln_1931/EN/PressSection/Publications/publications_node.html.

2009–2010. Broadband service, defined as a connection speed of at least 1 Mbps, is almost universally available.[2] However, in 2010 only 49.6 percent of the population actually used broadband service.[3]

Private ownership of computers and home internet connections are the norm. The 1990s privatization of the telecommunications sector in Germany has led to a stark drop in prices.[4] Current flat rates for internet service are below €24 (US$30) per month.[5] In addition, users can take advantage of free access at public institutions like libraries. Nevertheless, a sizeable share of the population makes little or no use of computers or the internet, whether out of lack of interest or lack of computer literacy.

Thanks to school-related access, 97.5 percent of all students aged 14 to 19 are internet users. Underprivileged groups are less likely to use the internet; they include women, older people, people with less formal education and less income, residents of the eastern states (formerly under communist rule) or very small cities, and people living alone.[6] Only 26 percent of the population uses the internet routinely and in a substantial way, and members of this group are typically male and 36 years old or younger.[7]

The video-sharing site YouTube, the Facebook social-networking site, the microblogging service Twitter, and international blog-hosting platforms are freely available. However, the four mobile-telephony providers in Germany prohibit in their general terms and conditions internet-based services, such as Voice over Internet Protocol (VoIP) and instant messaging, that would threaten their revenue from the equivalent telephony-based services. While these prohibitions have apparently not been enforced, their legality is questionable.[8] Similarly, the private ISP Kabel Deutschland was found in 2008 to have slowed down its connections during certain times of the day, which adversely affected users of the video-sharing technology BitTorrent in particular.[9] Such practices raise questions about the protection of net neutrality, which is coupled with the protection of telecommunications secrecy laid down in Section 88 of the Telecommunications Act.

The privatization of the telecommunications sector was undertaken with the aim of fostering competition. However, the market has become concentrated in the hands of a few

[2] Bundesministerium für Wirtschaft und Technologie [Federal Ministry of Economics and Technology, BMWi], *Breitbandatlas 2009_2* (Berlin: BMWi, 2009), 7, available at: http://www.zukunft-breitband.de/BBA/Navigation/Service/publikationen,did=303750.html (in German).
[3] Initiative D21, *(N)Onliner Atlas 2010* (Berlin: Initiative D21, 2010), 10, available at http://www.initiative21.de/category/nonliner-atlas/nonliner-atlas-2010 (in German).
[4] Bundesnetzagentur, *Annual Report 2009*.
[5] See, for instance, http://telko.check24.de or http://www.dslweb.de.
[6] Initiative D21, *(N)Onliner Atlas 2010*, 42.
[7] Initiative D21, *Digitale Gesellschaft: Die digitale Gesellschaft in Deutschland—Sechs Nutzertypen im Vergleich* (Berlin: Initiative D21, 2010), http://www.initiative21.de/wp-content/uploads/2010/03/Digitale-Gesellschaft_Endfassung.pdf (in German).
[8] Christoph H. Hochstätter, "Lauschangriff DPI: So hören die Provider ihre Kunden ab," ZDNet.de, March 24, 2009, http://www.zdnet.de/sicherheits_analysen_lauschangriff_dpi_so_hoeren_die_provider_ihre_kunden_ab_story-39001544-41001975-1.htm (in German).
[9] Janko Röttgers, "Internetanbieter bremst Taschbörsen aus," Focus Online, March 6, 2008, http://www.focus.de/digital/internet/kabel-deutschland_aid_264070.html (in German).

large companies over the past decade. The emerging leaders among ISPs and backbone internet providers are Deutsche Telekom, Arcor, United Internet, Freenet, QSC, Versatel, Telefónica, and AOL; many small ISPs have been forced out of business.[10] The country's four large mobile-phone companies are T-Mobile, E-Plus Mobilfunk, Telefónica O2, and Vodafone D2. Internet cafes are common in Germany, though their number may be decreasing amid growing individual computer ownership and the free wireless connections now offered in many bars and cafes. The main regulatory burdens faced by internet cafes relate to the protection of youth from harmful content and practices.[11]

ISPs must meet the technological and administrative requirements laid out in a decree on telecommunications interception before they can start doing business.[12] The entity responsible for regulating digital technology is the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (Bundesnetzagentur), operating under the auspices of the Federal Ministry of Economics and Technology. Its decisions, which are based on the Telecommunications Act, may be challenged directly before the administrative courts. Section 5(1) of the Federal Network Agency Act provides for an Advisory Council consisting of 16 members of the lower house of parliament and 16 representatives of the upper house, appointed by the federal government on the parliament's recommendation. The Advisory Council focuses on issues surrounding spectrum management, frequency usage, universal service obligations, and strategic policies of market relevance. [13] It also submits proposals to the federal government concerning the appointment of the president and the two vice presidents of the Federal Network Agency, who serve five-year terms and may be reappointed. They may also be dismissed if there is a serious reason to do so. The German Monopoly Commission has voiced the concern that this leaves the agency vulnerable to "political instrumentalization."[14] Separately, in 2010, the European Commission criticized the Federal Network Agency for passivity and the drawn-out nature of its regulatory procedures, which in practice might give a competitive

[10] See, for instance, the websites www.providersuche.org and www.teltarif.de/i/backbone.html.

[11] These mainly relate to online content, gaming, and the availability of alcohol in internet cafes. See Bundesprüfstelle für jugendgefährdende Medien [Federal Department for Media Harmful to Young Persons, BPjM], "Internetcafés: Rechtsauffassung der obersten Landesjugendbehörde zur jugendschutzrechtlichen Einordnung von gewerblichen Internetcafés," in *BPJM Aktuell 4* (Berlin: BPjM, 2005), http://www.bundespruefstelle.de/bpjm/redaktion/PDF-Anlagen/bpjm-aktuell-internetcafes-rechtsauffassung-der-oljb-aus-04-05,property=pdf,bereich=bpjm,sprache=de,rwb=true.pdf (in German).

[12] The decree's full title is "Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation." It is available at http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/gesamt.pdf (in German).

[13] Bundesnetzagentur, "Advisory Council," http://www.bundesnetzagentur.de/cln_1912/EN/FederalAgency/AdvisoryCouncil/advisorycouncil_node.html, accessed September 7, 2010.

[14] Monopolkommission [Monopoly Commission], *Telekommunication 2009: Klaren Wettbewerbskurs halten* (Berlin: Monopolkommission, 2009), 75, http://www.monopolkommission.de/sg_56/s56_volltext.pdf (in German). The European Commission has also taken up this concern. See 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.

advantage to Deutsche Telekom, the former state-owned monopoly.[15]

LIMITS ON CONTENT

The penal code contains provisions against certain types of public speech, most notably the propaganda of unconstitutional organizations (Section 86); hate speech, defamation, and calls for violence against segments of the population (Section 130); utterances that deny or render harmless acts committed under the rule of National Socialism and are capable of disturbing the public peace (Section 130); instructions for serious crimes (Section 130a); representations of violence against human beings that appear to glorify such violence or render it harmless, or that injure human dignity (Section 131); and pornography focused on acts of violence or sexual acts of human beings with animals (Section 184a) or with children under age 14 (Section 184b). Pornography in general is not forbidden, but it is illegal to give juveniles under age 18 access to it or facilitate their access to it (Section 184[1] and [2]). There are also laws prohibiting defamation, the divulging of state secrets, copyright violations, fraud (including phishing), spam, malware, and viruses.

Blocking is employed when illegal content is hosted abroad and entities in the host country are unwilling to remove it. While there is effective international collaboration on content removal with respect to problems like fraud,[16] extreme right-wing and neo-Nazi content is illegal in Germany but not in many other countries where it is hosted, meaning such material must be blocked in Germany.[17]

A new law restricting child pornography, signed in February 2010, has generated heated public debate. The measure requires ISPs to block access to pages containing child pornography, and authorizes the Federal Criminal Office (BKA) to compile continuously updated lists of the sites to be blocked. The law, which will only be in effect until the end of 2012, contains many legally questionable components, and has already fallen into so much disfavor that courts will reportedly not take it into consideration.[18] When the law was being drafted, a huge public campaign coordinated in large part by the Working Group Against Internet Blocks and Censorship recommended takedown notices and prosecution rather than blocking as an appropriate remedy.

---

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

[16] Tyler Moore and Richard Clayton, *The Impact of Incentives on Notice and Take-down* (Cambridge, UK: University of Cambridge, 2008), http://www.cl.cam.ac.uk/~rnc1/takedown.pdf.

[17] The blocking is hard to quantify, as there appears to be a great deal of fluctuation, with hundreds of extreme right-wing sites being blocked or taken down and hundreds of new ones surfacing each year. In 2007, for example, there were reportedly 250 new right-wing internet sites, and roughly the same number were deleted from the internet. Agence France-Presse, "SPD: Sperrung von 231 Internetseiten in öffentlichen Gebäuden," Focus Online, December 9, 2008, http://www.focus.de/politik/deutschland/spd-sperrung-von-231-internetseiten-in-oeffentlichen-gebaeuden_aid_354643.html (in German).

[18] Uwe Hessler, "German Child Pornography Law Hits Snags," Deutsche Welle, February 23, 2010, http://www.dw-world.de/dw/article/0,,5278471,00.html.

The role given to the BKA by the law was also criticized, with opponents arguing that content issues should be dealt with at the state level. Existing federal laws, such as the Telemedia Act and the Telecommunications Act, address general liability, data protection, and information transport, not content. Moreover, the BKA list is not open to the public and the procedures for checking its accuracy and challenging it directly appear inadequate. An independent expert group is tasked with drawing random samples from the list to determine whether the content is indeed child pornography. To appeal a listing, the website owner would have to go to administrative court.

Although there is a federal law addressing youth protection in different types of media, youth protection on the Internet is principally addressed by the states and their joint agreement on the topic, known as the Jugendmedienschutz-Staatsvertrag (JMStV).[19] Compliance with the JMStV, which outlaws content similar to that outlawed by the penal code, is overseen by the Commission for Youth Protection Relating to Media, which can ask the Federal Department for Media Harmful to Young Persons to put a website on its blacklist of youth-endangering media. Offending website owners residing in Germany are prosecuted, but if they are beyond the reach of German authorities, the blacklist is made available for integration into privately owned filtering software. Moreover, service providers have formed a voluntary self-regulation entity called the Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM), and participating search-engine companies have agreed to remove blacklisted websites from their search results.[20] Content that is forbidden to children but not to adults, such as adult pornography, must be made available in a way that verifies the age of the user.[21]

There is no censorship prior to publication. However, figures released by Google in 2010 on the number of requests for postpublication content removal by government entities seem to indicate that this strategy is used extensively in Germany. The country ranked second, behind Brazil, with 188 requests for removal between July 1, 2009, and December 31, 2009. Google complied fully or partially with 94.1 percent of these requests.[22] Notably,

[19] A revision of the JMStV was due to be adopted by the end of 2010, but eventually failed. It would have required each website hosted in Germany to include a tag like a movie rating specifying if its content should be restricted to certain age groups (e.g. six years and older, 12, 16 or 18 years and older). Critics of this revision conducted an experiment showing that even ratings specialists did not agree when trying to rate internet content, let alone any number of private individuals, who would under the new JMStV have to rate their own material. Further unresolved issues concerning this rating included liability and supervision issues and how to even apply such a provision to dynamic websites. See "Jugendmedienschutz-Novellierung endgültig gescheitert," *Heise Online* December 16, 2010, http://www.heise.de/newsticker/meldung/Jugendmedienschutz-Novellierung-endgueltig-gescheitert-1154880.html (in German).

[20] Currently, Google search results state how many hits have been removed for legal reasons, and offer a link to ChillingEffects.org for more information. Users who follow this link have to opportunity to compare the results for their search between Google.de and Google.com.

[21] BPjM, *BPJMThema Wegweiser Jugendmedienschutz: Ein Überblick über Aufgaben und Zuständigkeiten der Jugendmedienschutzinstitutionen in Deutschland* (Berlin: BPjM, 2009), http://www.bundespruefstelle.de/bpjm/redaktion/PDF-Anlagen/bpjm-thema-wegweiser-jugendmedienschutz,property=pdf,bereich=bpjm,sprache=de,rwb=true.pdf (in German).

[22] Google, "Transparency Report: Government Requests," http://www.google.com/governmentrequests/, accessed September 7, 2010.

other European countries logged far fewer requests; the only ones with more than 10 were Britain (59), Italy (57), and Spain (32). According to the German news website *Spiegel Online*, the content at issue in the German requests was mainly defamation, Holocaust denial, and unconstitutional neo-Nazi material.[23] The Google figures do not include sites removed because of child pornography or copyright infringements, or removals that Google initiated based on its own policies, such as a rule against hate speech on its blog-hosting platform, Blogger.[24]

Paragraph 8 of the Telemedia Act expressly states that access providers are not legally responsible for their customers' content unless they collaborate with users in breaking the law. However, courts have continued to disagree on whether web-hosting businesses and access providers can be made liable under the concept of *Störerhaftung* (liability of the interferer), defined in the civil code (for example in Sections 862 and 1004) as interference with the property of others. This concept has been invoked with respect to intellectual-property rights, business competition, and personality rights, among other topics.

A 2009 decision by a state court in Hamburg controversially extended the concept of *Störerhaftung* from web-hosting services to access providers. The access provider Hansenet/Alice had asked the court whether it was obliged to block access to websites with illegal content. While the court ruled that Hansenet/Alice could not "reasonably" be required to block, it based its verdict not on Paragraph 8 of the Telemedia Act, but on the view that the available blocking technology would only have a limited effect. Critics of the ruling argued that it would oblige access providers to block once effective means have been put in place.[25] The types of notification required to trigger the liability of the provider also remained uncertain, as did the extent to which providers could be sued by customers for improperly blocking or removing their content.

Germany is home to a vibrant web community and blogosphere, though the disproportionately young and male population of active users probably affects the mix of topics that are discussed. A great deal of attention is given to telecommunications and internet policies in general, and censorship and surveillance/data-retention issues in particular. A broad public protest against internet censorship in mid-2009 united hackers and digital activists with mainstream bloggers and Twitter users. The protesters launched an e-Petition, which was quickly signed by more than 130,000 people.[26]

[23] "Google-Statistik: Wie die Deutschen Zensur-Vizeweltmeister wurden," *Spiegel Online*, April 21, 2010, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,690278,00.html (in German).
[24] See Google, "Government Requests FAQ," http://www.google.com/governmentrequests/faq.html, accessed September 7, 2010.
[25] Holger Bleich, "Geplante Kinderporno-Sperre könnte andere Sperrverfügungen erleichtern," *Heise Online*, May 14, 2009, http://www.heise.de/newsticker/meldung/Geplante-Kinderporno-Sperre-koennte-andere-Sperrverfuegungen-erleichtern-219091.html (in German).
[26] Markus Beckedahl, "The Dawning of Internet Censorship in Germany," Global Voices Advocacy, June 16, 2009, http://advocacy.globalvoicesonline.org/2009/06/16/the-dawning-of-internet-censorship-in-germany/.

VIOLATIONS OF USER RIGHTS

The German Basic Law safeguards freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). While these articles have also set the standard for the online world, a groundbreaking 2008 ruling by the Federal Constitutional Court declared that the general right of personality guaranteed by Article 2 of the Basic Law "encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems."[27] Unfortunately, these rights have increasingly been contested in a trend that began even before the September 2001 terrorist attacks on the United States.[28] This is particularly worrying with respect to the rights of journalists. Like the clergy, defense lawyers, attorneys, counselors, and various categories of politicians, journalists have been accorded special standing by Paragraph 53 (1) 5 of the code of criminal procedure, which grants them the right to refuse to give evidence. However, the 2001 Act for Limiting the Secrecy of Letters, the Post, and Telecommunications (Article 10 Act–G 10) enables secret services to intercept, monitor, and record private communications, and it differentiates between the protected professions, allowing surveillance of counselors and journalists if the public interest in using their information to combat serious crimes outweighs the public interest in the performance of their professional tasks.

There have been a series of cases in which journalists' rights have been violated. In 2008, it was revealed that the Federal Intelligence Agency (BND) had been following e-mail exchanges between an Afghan politician and an editor at the German weekly *Der Spiegel* for months. The chairman of the Parliamentary Control Panel for the BND at the time voiced his disappointment that the agency had not adopted a stricter attitude toward such matters in the wake of similar scandals in 2006.[29] In fact, a Constitutional Court ruling in February 2007 had set a strong precedent for the protection of journalists' sources.[30] It declared criminal investigations against journalists unconstitutional if the whole or main aim was to

[27] Bundesverfassungsgericht [Federal Constitutional Court], Headnotes to the Judgment of the First Senate of 27 February 2008 on the basis of the oral hearing of 10 October 2007—1BvR 370, 595/07, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html.

[28] Even the Europe-wide security responses to the 2001 terrorist attacks may be seen as the seamless continuation of an existing trend toward increased surveillance. 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), http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

[29] "German Spies Caught Reading Journalist's E-Mails," Deutsche Welle, April 21, 2008, http://www.dw-world.de/dw/article/0,,3280594,00.html.

[30] Miklós Haraszti, *Access to Information by the Media in the OSCE Region: Trends and Recommendations: Summary of Preliminary Results of the Survey* (Vienna: Organization for Security and Cooperation in Europe, April 30, 2007), 11, http://www.osce.org/documents/rfm/2007/05/24250_en.pdf.

uncover the names of their informants. It further stated that the publication of a functional secret is not sufficient grounds for searching and seizing a journalist's property.[31]

In addition to police authorities and secret services, private companies including the airline Lufthansa and Deutsche Telekom have spied on journalists to identify their sources.[32] In 2008, Deutsche Telekom was found to have abused several hundred thousand sets of telephone traffic data, both landline and mobile, pertaining to journalists, board members, and others, with the goal of tracing information leaks within its ranks.[33] The company had apparently even employed a private detective agency to scan all news on Deutsche Telekom between January 2005 and March 2006 and create a list of journalists to be spied on because they apparently had access to confidential internal information.[34] The company itself acknowledged the "criminal energy" and "methodical malice" apparent in this affair.[35] At the time of writing, the trial had just started, but officials had already been criticized for failing to charge the then chairman of the company's supervisory board and the chief executive, and for delays in the release of crucial information to victims and plaintiffs.[36]

A substantial number of cases involving large companies and their questionable methods of gathering and using data have preoccupied the courts and the public in recent years. For instance, a 2008 case centered on the supermarket chain Lidl, which had comprehensively spied on its employees.[37] In the wake of scandals like these, an amendment to the Federal Data Protection Act was adopted in 2009, adding many provisions to strengthen employees' and users' rights regarding surveillance and unauthorized use of their data.[38] The latest debates on privacy and the practices of internet companies have revolved around Facebook and Google's Street View feature.[39]

While anonymous e-mail services, wireless internet-access points, and public telephone booths have remained legal, mobile-phone users who buy a new contract or

[31] Decision 1 BvR 538/06, 1 BvR 2045/06, February 27, 2007. For the larger European context, see Banisar, *Speaking of Terror*, 15 ff.

[32] "Lufthansa nutzt Passagierdaten für Überwachung," Netzpolitik.org, June 7, 2008, http://www.netzpolitik.org/2008/lufthansa-nutzt-passagierdaten-fuer-ueberwachung/ (in German).

[33] "Telekom bespitzelte Aufsichtsräte, Manager und Journalisten," *Spiegel Online*, May 24, 2008, http://www.spiegel.de/wirtschaft/0,1518,555148,00.html (in German).

[34] "Konzern beauftragte eine Detektei und bespitzelte diverse Reporter," UMTSlink, September 13, 2010, http://www.umtslink.at/3g-forum/news/63161-deutsche-telekom-bespitzelungsaffaere.html (in German).

[35] Deutsche Telekom, "Deutsche Telekom analysiert Tätikeit der früheren Konzernsicherheit," news release, February 10, 2010, http://www.telekom.com/dtag/cms/content/dt/de/812936?printversion=true (in German).

[36] "Telekom-Bespitzelungsaffaire: Journalisten wehren sich gegen Einstellung des Verfahrens," Golem.de, June 28, 2010, http://www.golem.de/1006/76063.html (in German).

[37] See, for instance, Anselm Waldermann, "Spitzel-Skandal: Lidl entschuldigt sich für Stasi-Methoden," *Spiegel Online*, March 26, 2008, http://www.spiegel.de/wirtschaft/0,1518,543597,00.html (in German).

[38] For a summary, see for instance Rhein Main Treuhand, "Datenschutz 2009 Verschärfung und Sanktion," http://www.rhein-main-treuhand.de/aktuelles/200911-datenschutz-2009-verschaerfung-und-sanktion.html (in German), accessed September 13, 2010.

[39] On Facebook, see for instance Maggie Shiels, "Germany Officials Launch Legal Action Against Facebook," British Broadcasting Corporation (BBC), July 8, 2010, http://news.bbc.co.uk/2/hi/8798906.stm. On Google Street View, see Ingo Ruhmann, "Google Street View: Eine politische Kampfansage," *Telepolis*, August 16, 2010, http://www.heise.de/tp/r4/artikel/33/33135/1.html (in German).

prepaid SIM (subscriber identity module) card must register with the network provider. The provider in turn is required to store the user's telephone number, name, address, and birth date; the start date of the contract; and, if applicable, the serial number of the mobile phone for the authorities.[40] Still, a mobile-phone user can achieve anonymity by buying the phone and phone number secondhand, because only the initial user needs to register.[41] Encryption software is freely available and may be used without restrictions.[42]

Law enforcement agencies and prosecutors can obtain users' contractual data without a judge's order under Sections 112 and 113 of the Telecommunications Act. However, judicial approval is required to obtain traffic and content data under Section 113 of the Telecommunications Act and Section 110g of the code of criminal procedure.[43] The Federal Network Agency serves as the data-collection intermediary standing between telecommunications companies and law enforcement bodies, fielding information requests from the latter. The less-protected contractual data is handled automatically, and for the year 2009, the agency reported 4.5 million requests from the authorities and 31.5 million queries directed to telecommunications-service providers.[44] A much smaller number of government entities are authorized, for more narrowly circumscribed purposes, to request more sensitive data under Section 113 of the Telecommunications Act. This data may include personal identity numbers (PINs) and personal unblocking keys (PUKs) that allow access to private terminals or web-based memory-hosting platforms, though the inquiries may only be used to identify the person who generated a certain communication or connection at a certain point in time. The number of requests for these breaches of telecommunications secrecy is reportedly 10 times lower than the number of automated requests for contractual data.[45] However, this would still amount to almost half a million requests in 2009.

Telecommunications interception by state authorities is regulated in Section 100 of the code of criminal procedure, or Strafprozessordnung (StPO). It is understood as a serious interference with basic rights and is subject to proportionality, meaning it may only be employed for the prevention or prosecution of very serious crimes for which specific evidence exists and for which other, less intrusive investigative methods will likely fail.

[40] This is required by Section 111 of the Telecommunications Act and applies to e-mail providers as well. However, it is not specified whether the telecommunications-service providers are required to verify their customers' information.
[41] Torsten Kleinz, "Handy-wechsel-dich," Zeit Online, April 25, 2008, http://www.zeit.de/online/2008/03/handykartenboerse (in German).
[42] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [Federal Commissioner for Data Protection and Freedom of Information], *Orientierungshilfe zum Einsatz kryptografischer Verfahren* (Berlin: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, September 2003), http://www.bfdi.bund.de/cae/servlet/contentblob/417366/publicationFile/25259/OrientierungshilfeZumEinsatzKryptografischerVerfahren.pdf;jsessionid=9348094A97AEA15E9D4F6C729361CB6A (in German).
[43] Alexander Schultz, "Auskunftsersuchen der Strafverfolgungsbehörden," Mediendelikte.de, http://www.mediendelikte.de/auskunftsersuchen.htm (in German), accessed September 13, 2010.
[44] The period from 2001 to 2009 shows a steady increase on both counts, from an initial 1.5 million requests from authorities and 3.2 million queries by the Federal Network Agency in 2001. Bundesnetzagentur, *Annual Report 2009*, 125.
[45] Kleinz, "Handy-wechsel-dich."

According to the most recent statistics published by the Federal Office of Justice, in 2008 there were a total of 16,463 orders for telecommunications interception based on Section 100a of the StPO. These referred to fixed-line phones in 3,821 cases, mobile phones in 13,838 cases, and internet communications in 661 cases.[46] Also in 2008, there were a total of 13,904 orders asking for traffic data based on Section 100g of the StPO and Sections 96 (1) and 113a of the Telecommunications Act.[47]

German authorities do not limit themselves to domestic data but also harvest data abroad. In March 2009, *Der Spiegel* reported that the BND had in previous years committed at least 2,500 acts of espionage by remotely searching computers abroad. These searches had at times included the undercover copying of hard drives and transmission of the data to Germany. In other cases they involved the installation of key loggers, which made it possible to track computer keystrokes and thereby gain access to passwords. Among the targets were Pakistani nuclear scientist Abdul Qadir Khan and the Iraqi government's computer system. German agents had also followed the e-mail traffic of an office run by the Welthungerhilfe aid group in Afghanistan. And as noted above, it was revealed in 2008 that the BND had for several months been illegally monitoring e-mail exchanges between Afghan government minister Amin Farhang and a *Spiegel* journalist.[48]

The generalized authority claimed by the BND, whose interceptions are supervised by the parliament's G 10 Commission rather than the judiciary,[49] was seen as particularly excessive at the time because of the landmark February 2008 decision by the Federal Constitutional Court on preventive covert remote computer searches. In its ruling, the court specified that such searches were only permissible "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 decision also ruled that any secret infiltration of an information-technology system is "in principle to be placed under the reservation of a judicial order," and that any statute permitting such an infiltration must "contain precautions in order to protect the core area of private life." Even more remarkably, as mentioned above, the court found that the general right of personality

[46] Some orders referred to more than one type of telecommunications interception. Bundesamt für Justiz [Federal Office for Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2008," July 14, 2009, http://www.bundesjustizamt.de/cln_108/nn_1635504/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/downloads/Uebersicht__TKUE__2008,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2008.pdf (in German).

[47] Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2008," August 24, 2009, http://www.bundesjustizamt.de/cln_115/nn_1635504/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/downloads/Uebersicht__Verkehrsdaten__2008,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2008.pdf (in German).

[48] Holger Stark, "Online-Durchsuchung: BND infiltrierte Tausende Computer im Ausland," *Spiegel Online*, March 7, 2009, http://www.spiegel.de/netzwelt/web/0,1518,611954,00.html (in German).

[49] Daniel Brössler, "Telefonüberwachung: Der Staat hört mit," Sueddeutsche.de, September 22, 2009, http://www.sueddeutsche.de/politik/2.220/telefonueberwachung-der-staat-hoert-mit-1.25048 (in German); Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10), available at http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf (in German), accessed September 9, 2010.

guaranteed by Article 2 of the German Basic Law "encompasses the fundamental right to the guarantee of the confidentiality and integrity of information-technology systems."[50]

A law that took effect in January 2009 empowered the BKA to conduct covert remote computer searches to prevent terrorist attacks with a judge's permission.[51] Online searches are also an option in very severe criminal cases, with a special responsibility to safeguard the individual's private life and the sensitive data obtained in the search. The law provides immunity from covert remote computer searches to political representatives, the clergy, and defense lawyers, but does not similarly protect doctors and journalists. In addition to computer searches, the act empowers 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. So far, the Federal Criminal Court has not availed itself of its new rights.[52] The state government of Rhineland-Palatinate empowered its police force in a similar way, adding the right to interrupt or hinder telecommunications but comprehensively protecting all the professional groups discussed above.

Preventive covert remote computer searches have been defended as a last-resort measure for combating terrorism, but the utility of the tactic has not yet been proven.[53] It has so far been ruled out as a source of evidence for criminal prosecution, and it remains unclear whether it may be used by secret services such as the BND, the Federal and State Offices for the Protection of the Constitution, and the Military Counterintelligence Service (MAD).

Since 1999, the BKA has maintained the Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD), roughly translating as a "central unit for unprovoked searches in data networks."[54] The ZaRD, rather than assisting with existing investigations or pursuing outside tips, actively monitors the internet for signs of unlawful activity in Germany and abroad. Once it has discovered such signs, it can request additional data under Section 113 of the Telecommunications Act, Sections 100g and 100h of the StPO, and Section 7 of the Federal Criminal Office Act, which in turn refers to Section 163 of the

[50] Bundesverfassungsgericht, Headnotes.

[51] 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).

[52] Cordula Eubel, "Online-Durchsuchungen – bisher geht es auch ohne," *Der Tagesspiegel*, May 25, 2010, http://www.tagesspiegel.de/politik/online-durchsuchungen-bisher-geht-es-auch-ohne/1844734.html (in German).

[53] It is interesting to note that the same was said about telecommunications interception at the 66th Conference of Federal and State Commissioners for Data Protection, held in Leipzig on September 25–26, 2003. See "Entschließung – Konsequenzen aus der Untersuchung des Max-Planck-Instituts für Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation," http://www.bfdi.bund.de/cae/servlet/contentblob/416440/publicationFile/25103/66DSK-KonsequenzenAusDerUntersuchungDesMax-Planck-InstitutsUeberRechtswirklichkeitUndEffizienzDerUeberwachungDerTelekommunikation.pdf (in German), accessed September 9, 2010.

[54] Its profile can be found at http://www.bka.de/profil/zentralstellen/zard.html (in German), accessed September 9, 2010.

StPO. The ZaRD's investigations uncover 600 to 800 cases of illegal activities annually, of which 70 percent or more involve the storage and dissemination of child pornography.[55]

The BKA reported a total of 50,254 criminal cases in 2009 involving information and communication technologies (ICTs), causing €36.9 million in damages. Almost half of the cases, 22,963, involved computer fraud, and the second-most-common type, at 11,491, centered on illegal data interception and spying.[56] The BKA noted that many more cases are not pursued legally or are not even detected, and that the professional perpetrators, especially international criminal syndicates, constitute a fundamental threat. This argument has been bolstered by the Association for German Criminal Investigators, which sees the internet as the "biggest crime scene of the world."[57] Among other steps, the association calls for mandatory registration with a governmental authority of every user who employs the internet for business transactions, the training of special units to fight computer crimes, and more scope for overt and covert investigations on the internet, especially on social-networking sites.

As of early 2009 there were a total of 80 surveillance facilities maintained by 38 different authorities in Germany. By midyear, a Telecommunications Surveillance Service Center and a Telecommunications Surveillance Competence Center had opened at the Federal Administration Office (Bundesverwaltungsamt) to support the existing surveillance facilities and to start centralizing their activities. The first step in this direction was the linking of the surveillance technologies of the BKA and the Federal Police that year. Critics argued that there was no legal basis for building such "super interception headquarters," and that they would erode the barrier between secret services and police that was incorporated into the constitution as one of the lessons learned from the Nazi era. Moreover, it was unclear how such a centralization of surveillance would safeguard the separation of different investigations and their distinct aims, legal underpinnings, and pools of data.[58]

As noted above, the secret services conduct surveillance under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications (Article 10 Act–G 10), which enables them to intercept, monitor, and record private communications, and stipulates that their activities are to be governed by the Parliamentary Control Panel, which in turn

[55] An indication of the constancy of this low number of cases and the prevalence of child pornography is provided by Robin O. Debie, "IuK-Kriminalität, mehr als nur Cybercrime: Entwicklung – Stand – Perspektiven," JurPC, 2004, available at http://www.jurpc.de/aufsatz/20040214.html (in German).

[56] Bundeskriminalamt [Federal Criminal Office], *IuK-Kriminalität: Bundeslagebild 2009* (Berlin: Bundeskriminalamt, 2010), 5, http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf (in German).

[57] Mirko Schubert , „Sicherheit: Kriminalbeamte fordern Notschalter für das Internet," *Netzwelt* (2010), http://www.netzwelt.de/news/83381-sicherheit-kriminalbeamte-fordern-notschalter-internet.html (in German), accessed January 20, 2011.

[58] These points are summarized in two online articles: Klaus C. Koch, "Telekommunikationsüberwachung: Feind hört mit," Sueddeutsche.de, September 14, 2009, http://www.sueddeutsche.de/digital/telekommunikationsueberwachung-feind-hoert-mit-1.28782 (in German); "Superabhörzentral in Köln ohne gesetzliche Grundlage: Datenschützer Peter Schaar kritisiert Bundesverwaltungsamt," Golem.de, August 4, 2009, http://www.golem.de/0908/68812.html (in German).

nominates the members of the G 10 Commission.[59] The latter assesses the necessity of telecommunications surveillance and controls the whole surveillance process. Its chairperson must have the qualifications to serve as a judge. The G 10 Commission is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Counterterrorism Amendment Act of 2007. The Parliamentary Control Panel reports periodically to the parliament about the activities of the G 10 Commission and, by extension, of the secret services.[60]

Data retention requirements apply to ISPs and mobile-phone companies, but not to internet cafes. The Federal Constitutional Court struck down a central law on data retention in March 2010, leaving a great deal of uncertainty on this issue.[61] The Law for the New Regulation of Telecommunications Interception and Other Covert Methods of Investigation as well as Compliance with the European Union Directive 2006/24/EG, which took effect in January 2008, had been challenged by more than 30,000 people, including Justice Minister Sabine Leutheusser-Schnarrenberg.[62] It was partly incorporated into the Telecommunications Act, and required telecommunications and internet providers to store all traffic data for six months. The court ruling ordered the deletion of this data. The court argued that the law was unconstitutional because it did not contain any specific measures to keep the data safe and failed to erect enough hurdles for accessing the information. However, the court left open the possibility that a data-retention law could be constitutional, so long as it was limited to facilitating the prosecution of clearly delineated, serious criminal offenses. There would also need to be "transparent control" over what the data could be used for,[63] and the law would have to establish strict procedures to be implemented by telecommunications providers.[64]

Cyberattacks are becoming an important issue in Germany. Citing the private security company G Data, the BKA report for 2009 stated that 350,000 to 700,000 computers—hijacked by hackers and organized into so-called botnets—were put to

[59] See the description on the website of the German parliament, http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html (in German).
[60] See the two briefings by the Parliamentary Control Panel to the parliament in 2010 (Drucksache 17/549 on the measures relating to the Article 10 Act and Drucksache 17/550 on the measures relating to the Counterterrorism Act), both covering the year 2008, available at http://dipbt.bundestag.de/dip21/btd/17/005/1700549.pdf and http://dipbt.bundestag.de/dip21/btd/17/005/1700550.pdf (in German), accessed September 13, 2010.
[61] Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08; verdict available at http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (in German), accessed September 13, 2010.
[62] Privacy International, "German Federal Constitutional Court Overturns Law on Data Retention," news release, March 9, 2010, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566038.
[63] It was along these lines that the Federal Constitutional Court limited the use of the law on March 11, 2008, after it received the first formal complaints. Bundesverfassungsgericht, "Eilantrag in Sachen 'Vorratsdatenspeicherung' teilweise erfolgreich," news release, March 19, 2008, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-037.html (in German).
[64] Bundesverfassungsgericht, "Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß," news release, March 2, 2010, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011 (in German).

fraudulent use every day in Germany.[65] G Data also enumerated several major cyberattacks for the first half of 2010.[66] For instance, in January, the website of the German Agency for Emissions Trading was subjected to a phishing attack, in the course of which emission allowances were illegally transferred to Denmark and Britain and the perpetrators made up to €3 million. In February, German online news portals such as Golem.de, Handelsblatt.com, and Zeit.de became victims of "malvertising," in which malicious code was downloaded onto the computers of site visitors through infected advertisement banners. In March, the website of the Federal Environment Agency was infected and spread a Zeus Trojan virus for several days. And in May, the data of more than two million students was stolen from the social-networking platform SchülerVZ, apparently in an attempt to alert the site to its security failures.

The German government created the Federal Office for Information Security (BSI) in 1991 to strengthen the security of federal information technology. The act that established the BSI was amended in 2009,[67] giving more leeway to the entity, which has 500 employees. A constitutional complaint has been directed against a paragraph in the amended act that allegedly allows the office to engage in massive data-retention activities.[68]

[65] Bundeskriminalamt, *IuK-Kriminalität: Bundeslagebild 2009*, 10. These numbers should perhaps be viewed with some caution, given that a private provider of security services has an interest in portraying computer crime as a pervasive threat.
[66] G Data issues semiannual malware reports. See Ralf Benzmüller and Sabrina Berkenkopf, *G Data Malware-Report: Halbjahresbericht Januar–Juni 2010* (Bochum: G Data, 2010), http://www.gdata.de/uploads/media/GData_MalwareReport_2010_1_6_DE_mail2.pdf (in German).
[67] Bundesministerium des Innern [Federal Ministry of the Interior], "Act to Strengthen the Security of Federal Information Technology," August 14, 2009, http://www.bmi.bund.de/cln_183/sid_4F946AA4F22A39F6785D8D2AE5F723D9/SharedDocs/Downloads/EN/Gesetzestexte/bsi_act.html?nn=105406.
[68] "Verfassungsbeschwerde gegen BSI-Gesetz eingereicht," Heise Online, September 1, 2010, http://www.heise.de/newsticker/meldung/Verfassungsbeschwerde-gegen-BSI-Gesetz-eingereicht-1070391.html (in German).