

## Germany

Germany is a country of high Internet penetration, at approximately 76 percent. Occasionally, takedown requests and access restrictions are imposed on ISPs, usually with the justification of protecting minors or in compliance with Germany’s objective to suppress hate speech and extremism. In April 2009, the German government signed a bill that would implement large-scale filtering of child pornography Web sites, with the possibility for later expansion. Additionally, the German government recently approved draft legislation to implement data retention.



### Background

After World War II, Germany was divided into American, British, French, and Russian zones. The Federal Republic of Germany (West Germany), a federal parliamentary republic, was founded in 1949 out of the three Western zones. The German Democratic Republic (East Germany), an authoritarian socialist state, was established in the Russian zone. In both states, continuing to uphold the obligations of Germany’s history and preventing a repetition of extremism have been a priority ever since. In

#### RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political	•				
Social	•				
Conflict and security	•				
Internet tools	•				

Other Factors	Low	Medium	High	Not Applicable
Transparency				•
Consistency				•

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	33,181
Life expectancy at birth (years)	80
Literacy rate (percent of people age 15+)	99
Human development index (out of 179)	23
Rule of law (out of 211)	12
Voice and accountability (out of 209)	11
Democracy index (out of 167)	13 (Full democracy)
Digital opportunity index (out of 181)	19
Internet users (percent of population)	76

Source by indicator: World Bank 2009a, World Bank 2009a, World Bank 2009a, UNDP 2008, World Bank 2009b, World Bank 2009b, Economist Intelligence Unit 2008, ITU 2007, ITU 2008.

1990, East Germany joined the Federal Republic of Germany. Since that time, reconciling economic differences has shaped German policy.

In 1949, West Germany adopted its “Basic Law” (*Grundgesetz*)—similar to a constitution—which provides for freedom of expression; however, the Basic Law also restricts expression that is “offensive, injurious, or indecent.”<sup>1</sup> Germany maintains a blacklist of books, comic books, magazines, videotapes, and music, the so-called *Index*. The list, originally intended to shield youth from pornographic material, has been expanded to include other items; in particular, materials that make light of Germany’s history and those which promote neo-Nazism or deny the Holocaust have been blacklisted.<sup>2</sup> *Volksverhetzung*, defined in Germany as “incitement of hatred against a minority under certain conditions,” is also strictly prohibited and punishable with up to five years’ imprisonment.<sup>3</sup>

### Internet in Germany

The Internet is a central part of the German economy. Over the past ten years, fierce competition has led to low prices and fueled Internet access. In 2008, Internet penetration stood at approximately 76 percent.<sup>4</sup> Germany’s primary ISPs are T-Online (47 percent market share), United Internet (15 percent), AOL (12 percent), and Arcor (7 percent).<sup>5</sup>

T-Online is a spin-off of Deutsche Telekom. Deutsche Telekom is the former state-run telecom, hence its high market share. Today, T-Online provides Internet services and software, while Deutsche Telekom maintains the physical connection. Deutsche Telekom still owns the majority of the physical network, including 90 percent of all existing broadband connections.

Broadband access in Germany has increased in recent years, from 200,000 in 2000 to 14.7 million in 2006. Because the service is inexpensive, this number is expected to rise

to 21.3 million in 2010.<sup>6</sup> In 2008, T-Online's DSL flat rate was EUR 10 (USD 15) per month.<sup>7</sup> Germany has 16 international Internet exchange points (IXP).<sup>8</sup> The largest one by far is the Deutsche Commercial Internet Exchange DE-CIX in Frankfurt, which is the second-largest IXP in the world with an average throughput of 200 Gbps and a maximum of more than 400 Gbps.<sup>9</sup>

### Legal and Regulatory Frameworks

The regulator for the telecommunication sector of the economy is the *Bundesnetzagentur* (Federal Network Agency), which is also responsible for the postal service and energy services.<sup>10</sup> It has been endowed with authority by the *Telekommunikationsgesetz* (TKG, Telecommunications Act) of 2004.<sup>11</sup>

The law that concerns the Internet as a medium is the *Telemediengesetz* (TMG, Telecommunication Media Law) passed by the parliament in January 2007.<sup>12</sup> Section 8 of the TMG explicitly states that providers are not responsible for transmitted information, provided they did not initiate the transmission or modify the transferred data.

The legal foundations for censorship are grounded in Germany's laws prohibiting public incitement of hatred against a minority (*Volksverhetzung*) and Holocaust denial. For example, Section 130(3) of the German Criminal Code notes, "Whoever . . . denies or renders harmless an act [of genocide] committed under the rule of National Socialism in a manner capable of disturbing the public peace shall be punished with imprisonment for not more than five years or a fine."<sup>13</sup> Additionally, media considered harmful to minors are regulated by the *Bundesprüfstelle für jugendgefährdende Medien* (BPjM, Federal Department for Media Harmful to Young Persons), which traditionally censored films, print media, and computer games, but has expanded its focus to the Internet.<sup>14</sup>

Because of the federal structure of Germany's political system, Internet censorship can be initiated at the regional level. In 2002, the *Bezirksregierung Düsseldorf* (district government) obliged 56 ISPs to restrict access to four foreign Web sites.<sup>15</sup> Each of these Web sites was based in the United States and contained right-wing extremist material.

The *Bezirksregierung*, which enforces the restrictions on Internet speech in the federal state of North Rhine–Westphalia, offered the ISPs a choice of three ways to implement the blockade: DNS-blockade, IP-blockade, or usage of a proxy server.<sup>16</sup> An online petition condemning these attempts to block access has received more than 26,000 signatures.<sup>17</sup> However, neither political demonstrations nor lawsuits have been successful in stopping the blockade. In the end, the administrative court of Düsseldorf endorsed the blockade in 2005.<sup>18</sup> By now, 76 Internet service providers have been required to block right-wing extremist Web sites.<sup>19</sup>

Furthermore, according to a study published by the Berkman Center for Internet and Society in 2002, a number of Web sites relating to neo-Nazi, white supremacist,

or other objectionable materials were completely or partly excluded by the German version of the search engine Google (google.de).<sup>20</sup>

While cases of blocking might occur infrequently, takedown requests, many of which receive a positive response, occur far more often. For example, as a result of the prohibition of Holocaust denial and public incitement of hatred against a minority in Germany, complaints have been filed against companies that host such content. The most prominent example is YouTube. In August 2007, German politicians and the Central Council of Jews in Germany complained about the extremist content that was being hosted on YouTube.<sup>21</sup> A YouTube spokesman promptly promised to improve the system of takedowns to comply with the demands of German law.<sup>22</sup>

A related issue is the political and judicial debate over whether linking to presumably illicit content is illegal. Several instances of this issue have been recorded. For example, in 2004 the political activist Alvar Freude was accused of linking to right-wing extremist Web sites and was brought to court. Freude had documented the censorship by the Düsseldorf district government mentioned previously and had linked to blocked Web sites. The district court found him guilty. However, Stuttgart Regional Court overturned that decision in 2006 and acquitted Freude.<sup>23</sup>

In another case involving prohibited online material, the Federal Court of Justice decided in 2000 that the Australian owner of an Australian Web site denying the Holocaust could be held liable in Germany.<sup>24</sup>

Another reason provided for Internet blocking is the protection of minors. The legal details are regulated in the *Jugendschutzgesetz* (JuSchG, Youth Protection Act)<sup>25</sup> and the *Jugendmedienschutz-Staatsvertrag* (JMStV, Youth Media Protection Treaty).<sup>26</sup> The JuSchG regulates *Trägermedien* (physical media) like books and videos. The JMStV regulates broadcasts and *Telemedien* (transmitted media) like the Internet.

More generally, Section 184(1) of the German Criminal Code states, “Whoever, in relation to pornographic writings . . . offers, gives or makes them accessible to a person under eighteen years of age . . . shall be punished with imprisonment for not more than one year or a fine.”<sup>27</sup> In addition, the dissemination of pornographic performances through electronic media is prohibited if the provider does not ensure by technical or other means that the performance is not accessible to persons under 18 years of age (Section 184d of the German Criminal Code). These laws are taken as a requirement for Web sites with adult content to implement a strict age verification system. For example, Flickr has complied with this perceived requirement by prohibiting German users from accessing photos marked “restricted.”<sup>28</sup>

Since the amendment of the JuSchG and JMStV in 2003, the BPjM has maintained a blacklist of Web sites. In order to avoid widespread publicity, this blacklist is not published. One may inquire as to whether an item is on the blacklist by e-mailing [liste@bundespruefstelle.de](mailto:liste@bundespruefstelle.de).<sup>29</sup> At the time of writing, the BPjM Web site stated that the number of censored Web sites was 1,948.<sup>30</sup>

In February 2005, Google Germany, Lycos Europe, MSN Germany, AOL Germany, Yahoo, and T-Online agreed to self-regulate their search results under the head of the *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* (FSM, Voluntary Self-Regulation of Multimedia Service Providers).<sup>31</sup> The FSM is a self-regulatory body for multimedia service providers funded by several Internet companies in 1997. One of the FSM's policies is to exclude Web sites that have been blacklisted by the BPjM from the search indices of its members. The current BPjM blacklist is regularly transferred to a hidden server; the search engines then download the list and automatically remove the relevant entries.

A number of cases have been brought to public attention. One in particular involves bmezzine.com, a Web site that "serves to document the activities of the body modification community."<sup>32</sup> In 2005, after BPjM judged the Web site to be a host of content harmful to minors, it required Google.de to remove BMEzzine from its search results.<sup>33</sup> A second incident occurred in late 2007, when German adult content providers sued several ISPs in various German states to block several Web sites that contained pornographic content.<sup>34</sup> The pages in question were hosted abroad and thus lacked a strict age verification system. The district court of Frankfurt ordered the respective defendant to block all relevant DNS addresses, while other courts dismissed the actions.<sup>35</sup> In particular, a request to block Google was dismissed.<sup>36</sup> Furthermore, the *Oberlandesgericht Frankfurt* (Higher State Court) confirmed another dismissal of a court of first instance, judging that ISPs could not be held liable for content that they only transmit.<sup>37</sup>

### Surveillance

Although Internet access remains mostly unrestricted in Germany, Internet users have recently been subject to state action. Germany's Criminal Procedure Code specifies in Section 100a that "the telecommunication of an individual may be monitored and recorded if:

1. Specific facts substantiate the suspicion that somebody was the perpetrator or participant in a serious crime as listed in paragraph 2 or, in cases where the attempt is liable to persecution, has attempted to commit such crime, or has prepared such crime by means of a criminal offense
2. The alleged crime would weigh heavily even taken individually
3. Investigating the act or determining the suspected person's location by other means would be significantly impeded or futile without surveillance"

Since January 2008, ISPs and online service providers in Germany have been required to retain certain data without initial suspicion of illegal activity (*Vorratsdatenspeicherung*).<sup>38</sup> The parliament passed the relevant law in November 2007,<sup>39</sup> which implements a European Union (EU) directive<sup>40</sup>; prior to its implementation, ISPs were

allowed to retain only data required for billing customers. The new law amends the *Telekommunikationsgesetz* (TKG). Section 113a specifies that providers of e-mail services must retain the following data:

- If a message is sent: the sender's e-mail and IP addresses, e-mail addresses of all recipients;
- If a message is received: e-mail address of the sender, e-mail address of the recipient, IP address of the sending server;
- If a client accesses his inbox: his e-mail address and IP address
- For all of the preceding: date, time, and time zone.

Internet service providers, however, must retain the following:

- IP address of the client;
- A unique identifier of the client's landline, allowing the identification of the client;
- Date and time of the beginning and end of the user's Internet access.

The data are then retained for six months. Section 113b establishes that the retained data may be used solely for the following purposes:

1. Prosecuting criminal acts;
2. Preventing substantial dangers to public safety;
3. Fulfilling the lawful obligations of Germany's intelligence offices.

An additional complaint has been filed at Germany's *Bundesverfassungsgericht* (Federal Constitutional Court) in December 2007, claiming that data retention is unconstitutional. In March 2008, the court issued an injunction to restrict data retention to exceptional cases. A final decision on data retention is still outstanding.

Whatever the final judgment may be, the last several years have displayed a clear trend toward increasing Internet surveillance. Motivating factors behind this development include the impetus to prevent terrorism, to prosecute crimes, and to enforce intellectual property rights.

Finally, the fear of terrorism and right-wing extremism has led not only to the monitoring of e-mails and chat rooms by the *Bundeskriminalamt* (Federal Criminal Police Office), but also to the idea of "online raids."<sup>41</sup> This involves infecting a suspect's personal computer with Trojan software, which records data entered in order to extract the relevant information clandestinely. However, online raids remain highly controversial. The federal constitutional court ruled in March 2008 that online raids may be used only in exceptional circumstances.<sup>42</sup>

### ONI Testing Results

In 2007 and 2008, the OpenNet Initiative conducted testing on T-Online, Arcor, and 1&1 and found no evidence of filtering, despite Germany's laws prohibiting certain

content. After ONI testing, however, the German government signed an agreement with five leading ISPs for the filtering of child pornography using DNS tampering.<sup>43</sup> Although the filters will initially target a list of approximately 1,000 child pornography sites, the Ministry of Family Affairs has stated that it could be expanded to include other content in the future.

## Conclusion

Currently, German users can access the Internet with only mild restrictions. However, the April 2009 filtering bill and the recent legislation on data retention could have a staggering effect on Web site access and Internet surveillance in the future. The decision to implement a large-scale filtering system follows in the footsteps of a number of other European nations, including the United Kingdom and Scandinavian countries, and could prove to be influential for other members of the EU.

## Notes

1. Robert Trager and Donna Lee Dickerson, *Freedom of Expression in the 21st Century* (Thousand Oaks: Pine Forge Press, 1999), 8.
2. *Ibid.*, 105.
3. *Strafgesetzbuch* [German Criminal Code], Section 130, [http://bundesrecht.juris.de/stgb/\\_130.html](http://bundesrecht.juris.de/stgb/_130.html).
4. International Telecommunications Union (ITU), "Internet Indicators: Subscribers, Users, and Broadband Subscribers," 2008, [http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP\\_intYear=2008&RP\\_intLanguageID=1](http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1).
5. *Rhein-Zeitung Online*, "HanseNet Greift Internetanbieter Deutschlandweit an" [HanseNet Attacks Internet Service Providers throughout Germany], June 30, 2005, <http://rhein-zeitung.de/on/05/07/19/service/multimedia/t/rzo163384.html>.
6. Bernd W. Wirtz, "Unser Leben im Netz" [Our Life Online], *Deutschland Online*, [http://www.studie-deutschland-online.de/do5/sdo\\_2007\\_de.pdf](http://www.studie-deutschland-online.de/do5/sdo_2007_de.pdf).
7. T-Online, "DSL Tarif," <http://www.dsl.t-online.de/c/12/42/10/20/12421020.html>.
8. European Exchange Points, [http://www.ep.net/naps\\_eu2.html](http://www.ep.net/naps_eu2.html).
9. DE-CIX German Internet Exchange, <http://www.de-cix.net/>.
10. *Bundesnetzagentur* [Federal Network Agency], <http://www.bundesnetzagentur.de/>.
11. *Bundesministerium der Justiz* [Federal Ministry of Justice], "Telekommunikationsgesetz" [Telecommunications Act], [http://www.gesetze-im-internet.de/tkg\\_2004/](http://www.gesetze-im-internet.de/tkg_2004/).

12. *Bundesministerium der Justiz* [Federal Ministry of Justice], “Telemediengesetz” [Telecommunication Media Act], <http://www.gesetze-im-internet.de/tmg/>.
13. German Criminal Code (*Strafgesetzbuch*), Section 130, [http://bundesrecht.juris.de/stgb/\\_130.html](http://bundesrecht.juris.de/stgb/_130.html).
14. *Bundesprüfstelle für Jugendgefährdende Medien* [Federal Department for Media Harmful to Young Persons], <http://www.bundespruefstelle.de/>.
15. *Heise Online*, “Nordrhein-westfälische Provider Sollen Nazi-Websites Ausfiltern” [Internet Service Providers in North Rhine–Westphalia are to Filter Nazi Web sites], October 8, 2001, <http://www.heise.de/newsticker/Nordrhein-westfaelische-Provider-sollen-Nazi-Websites-ausfiltern--/meldung/21627>.
16. *Sperrungsverfügung* [Blocking Order], <http://www.odem.org/material/verfuegung/>.
17. Internet-Zensur in Deutschland, “Sperrungen Sollen es Ihnen Unmöglich Machen, sich Tausende Internetseiten Anzuschauen” [Blockings Are to Prevent You from Accessing Thousands of Web sites], <http://odem.org/informationsfreiheit/en/>.
18. *Heise Online*, “Verwaltungsgericht Düsseldorf Bestätigt Sperrungsverfügung in NRW” [Administrative Court of Düsseldorf Confirmed the Blocking Order in North Rhine–Westphalia], <http://www.heise.de/newsticker/Verwaltungsgericht-Duesseldorf-bestaetigt-Sperrungsverfuegung-in-NRW--/meldung/60627>.
19. *Heise Online*, “Düsseldorfer Bezirksregierung Sieht sich Erfolgreich im Kampf Gegen Nazi-Websites” [Düsseldorf District Government Believes It is Successful in the Fight against Nazi Web sites], November 22, 2005, <http://www.heise.de/newsticker/Duesseldorfer-Bezirksregierung-sieht-sich-erfolgreich-im-Kampf-gegen-Nazi-Website--/meldung/66501/>.
20. Jonathan Zittrain and Benjamin Edelman, “Localized Google Search Result Exclusions: Statement of Issues and Call for Data,” Berkman Center for Internet and Society, Harvard Law School, October 26, 2002, <http://cyber.law.harvard.edu/filtering/google/>.
21. *Heise Online*, “Google Intends to Speed Up Removal of Far Right Content from YouTube,” August 31, 2007, <http://www.heise.de/english/newsticker/news/95230/from/rs09>.
22. Rubriken Stern, “YouTube: Nazis Raus!” [YouTube: Get the Nazis Out], August 29, 2007, <http://www.stern.de/wirtschaft/news/unternehmen/youtube-nazis-raus-596475.html>.
23. *Heise Online*, “Revisionsverhandlung Gegen Netzaktivisten Steht an” [Hearings Ahead in Internet Activist’s Appeal], April 19, 2006, <http://www.heise.de/newsticker/Revisionsverhandlung-gegen-Netzaktivisten-steht-a--/meldung/72134>.
24. Florian Rötzer, “Update: Leugnung des Holocaust im Internet nach Deutschem Recht Strafbar” [Update: Denial of the Holocaust on the Internet Punishable under German Law], “*Heise Online*,” December 13, 2000, <http://www.heise.de/tp/r4/artikel/4/4467/1.html>.
25. *Jugendschutzgesetz* [Youth Protection Act], January 1, 2009, <http://www.bmfsfj.de/Kategorien/gesetze,did=5350.html>.



26. *Jugendmedienschutz-Staatsvertrag* [Youth Media Protection Treaty], <http://www.artikel5.de/gesetze/jmstv.html>.
27. *Strafgesetzbuch*, StGB [German Criminal Code], "Section 184 Dissemination of Pornographic Writings," <http://www.iuscomp.org/gla/statutes/StGB.htm#184>.
28. Flickr, "Content Filters," <http://www.flickr.com/help/filters/#249>.
29. *Heise Online*, "Betreiber einer Piercing-Site Beklagt Deutsche Zensur," [Owner of Piercing Web site Complains about German Censorship], December 23, 2005, <http://www.heise.de/newsticker/Betreiber-einer-Piercing-Site-beklagt-deutsche-Zensur--/meldung/67716>.
30. Statistics of the *Bundesprüfstelle für Jugendgefährdende Medien* [Federal Department for Media Harmful to Young Persons], <http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/Jugendmedienschutz/statistik>.
31. *Heise Online*, "Selbstregulierung der Suchmaschinenanbieter" [Self-regulation of Search Engine Providers], February 24, 2005, <http://www.heise.de/newsticker/Selbstregulierung-der-Suchmaschinenanbiete--/meldung/56770>.
32. BMEZine, "Warning, Adult Notice, and Charter," <http://bmezine.com/why.html>.
33. *Heise Online*, "Betreiber einer Piercing-Site Beklagt Deutsche Zensur," [Owner of Piercing Web site Complains about German Censorship], December 23, 2005, <http://www.heise.de/newsticker/Betreiber-einer-Piercing-Site-beklagt-deutsche-Zensur--/meldung/67716>.
34. *Heise Online*, "Arcor Sperrt Zugriff auf Porno-Seiten" [Arcor Blocks Access to Porn Sites], September 10, 2007, <http://www.heise.de/newsticker/Arcor-sperret-Zugriff-auf-Porno-Seiten--/meldung/95758>. Note: among the sites involved were sex.com, YouPorn.com, and privatamateure.com.
35. *Heise Online*, "Arcor Muss YouPorn Sperren [Update]" [Arcor Has to Block YouPorn], October 19, 2007, <http://www.heise.de/newsticker/Arcor-muss-YouPorn-sperren-Update--/meldung/97676>; *Heise Online*, "Arcor hat Widerspruch Gegen Verfügung zur YouPorn-Sperre Eingelegt" [Arcor Appeals Against Order to Block YouPorn], November 22, 2007, <http://www.heise.de/newsticker/Arcor-hat-Widerspruch-gegen-Verfuegung-zur-YouPorn-Sperre-eingelegt--/meldung/99404>; *Heise Online*, "Weiterer Antrag auf Sperrung von Pornoseiten Zurückgewiesen" [Further Request to Block Porn Sites Rejected], December 13, 2007, <http://www.heise.de/newsticker/Weiterer-Antrag-auf-Sperrung-von-Pornoseiten-zurueckgewiesen--/meldung/100513>.
36. *Heise Online*, "Arcor soll Google Sperren" [Arcor Is to Block Google], December 4, 2007, <http://www.heise.de/newsticker/Arcor-soll-Google-sperren--/meldung/100035>.
37. *Heise Online*, "OLG: Provider Nicht für Netzinhalte Verantwortlich" [Higher State Court: Provider Is Not Responsible for Web Content], January 23, 2008, <http://www.heise.de/newsticker/OLG-Provider-nicht-fuer-Netzinhalte-verantwortlich--/meldung/102309>.
38. *Stoppt die Vorratsdatenspeicherung*, "5-Minute Overview: German Data Retention Law," <http://www.vorratsdatenspeicherung.de/content/view/46/1/lang,en/>.

39. The law is called the *Gesetz zur Neuregelung der Telekommunikationsüberwachung und Anderer Verdeckter Ermittlungsmaßnahmen Sowie zur Umsetzung der Richtlinie 2006/24/EG* [Law on the Revision of Telecommunications Surveillance and Other Covert Investigative Measures and to Implement the Directive].

40. "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>.

41. Katrin McGauran, "Germany: Permanent State of Pre-emption," *Statewatch Journal*, October–December 2008, <http://www.statewatch.org/analyses/no-79-germany-permanent-state-of-preemption.pdf>.

42. *BBC News*, "The Most Spied Upon People in Europe," February 28, 2008, <http://news.bbc.co.uk/2/hi/europe/7265212.stm>.

43. *Metamorphosis*, "German Government Forces ISPs to Put Web Filters," April 27, 2009, <http://www.metamorphosis.org.mk/edri/german-government-forces-isps-to-put-web-filters.html>.

This is a section of [doi:10.7551/mitpress/8551.001.0001](https://doi.org/10.7551/mitpress/8551.001.0001)

# Access Controlled

## The Shaping of Power, Rights, and Rule in Cyberspace

**Edited by:** Ronald Deibert, John Palfrey, Rafal Rohozinski,  
Jonathan L. Zittrain

### Citation:

*Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*

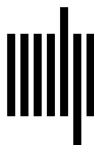
**Edited by:** Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

**DOI:** 10.7551/mitpress/8551.001.0001

**ISBN (electronic):** 9780262266031

**Publisher:** The MIT Press

**Published:** 2010



The MIT Press

© 2010 Massachusetts Institute of Technology

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

For information about special quantity discounts, please email [special\\_sales@mitpress.mit.edu](mailto:special_sales@mitpress.mit.edu)

This book was set in Stone Serif and Stone Sans on 3B2 by Asco Typesetters, Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access controlled : the shaping of power, rights, and rule in cyberspace / edited by Ronald Deibert . . . [et al.] ; foreword by Miklos Haraszti.

p. cm. — (Information revolution and global politics)

Report from the OpenNet Initiative.

Includes bibliographical references and index.

ISBN 978-0-262-01434-2 (hardcover : alk. paper) — ISBN 978-0-262-51435-4 (pbk. : alk. paper)

1. Cyberspace—Government policy. 2. Internet—Government policy. 3. Computers—Access control. 4. Internet—Censorship. I. Deibert, Ronald. II. OpenNet Initiative.

HM851.A254 2010

005.8—dc22

2009049632

10 9 8 7 6 5 4 3 2 1