# Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates*

18th July 2012

## Abstract

Liberal democracies are increasingly considering internet filtering as a means to assert state control over online information exchanges. A variety of filtering techniques have been implemented in Western states to prevent access to certain content deemed harmful. This development poses a series of democratic and ethical questions, particularly when states introduce regulation mandating ISPs to block online content. In this work we examine the debates surrounding filtering that have played out in two key European states, France and Germany, focusing on the arguments used by opponents and proponents of internet blocking. We use these to explain and analyse the outcomes of both cases and, more broadly, the various challenges posed by internet blocking to democracy.

## 1 Introduction

Research into internet filtering and censorship has typicaly focused on authoritarian regimes [3, 9, 11, 1]. However Western states, with a long-term commitment to fundamental rights, including freedom of expression, are increasingly debating and implementing internet filtering. Filtering is a new policy tool

---

for liberal democracies, and is increasingly becoming a global norm for asserting state sovereignty online [8, 21, 31]. The issue is more nuanced than whether or not the internet can and should be regulated. For liberal democracies, it is a question of finding the right balance between sometimes diverging principles, such as ensuring security and public safety without restricting other democratic principles such as freedom of expression and privacy.

In many Western societies, internet regulation is becoming an increasingly politicized issue. Contrary to authoritarian regimes, liberal democracies are subject both to the rule of law, and to democratic principles and norms including public debate. These principles are increasingly invoked and debated when states or corporations attempt to alter the flow of information through the internet. As a result, issues such as child abuse images, copyright, and network neutrality have become central to decision-makers, industry lobbyists, and contending social groups, many of whom resort extensively to digital communications to mobilize supporters [2, 19, 25].

Internet filtering takes the shape of self-, co- or state-regulatory arrangements. Finland, Sweden, Norway, Denmark, the UK, Italy, the US, Canada and New Zealand have all established a self-regulatory blocking system to prevent access to child abuse content. Australia has one of the most severe internet policies and practices of Western states [11]. However, a mandatory internet filtering policy has met opposition and been delayed repeatedly. Regulatory attempts at introducing internet filtering of child abuse images legislation in France, Germany and at the European Union level have equally encountered

strong opposition that resulted in the revocation and abandonment of the measure in Germany and the EU, not in France. Such state regulation offers a privileged moment of analysis to comprehend the framing of internet filtering in democracies. We assess internet filtering in terms of democratic principles such as accountability, legitimacy and transparency (§2). We then provide an original analysis of the debates surrounding the internet filtering measures in France and Germany (§3). We argue that internet filtering is increasingly contested, often successfully, when states choose legislative reform that allows for a variety of stakeholders to intervene in the policy-process. Self-regulatory mechanisms, however, largely evade public oversight and are thus questionable from a viewpoint of democratic principles.

## 2 Democratic principles and internet filtering

Filtering, or censorship, represents one of the more far-reaching and politically sensitive interactions between nation states and the internet. The assertion of state control over the internet is increasingly being shaped by technological solutions to political issues, as in Lessig's concept of 'code as law' [18]; by indirect enforcement through intermediaries; and by a tendency towards self-regulation over legislation [21]. The internet poses new challenges to regulation that have led to serious failures of traditional approaches as states attempted to legislate an unfamiliar and global medium [5]. It is thus not surprising that various forms of self-regulation have proven more successful than state-based approaches, especially when dealing with illegal content [16].

While the nature of filtering is undoubtedly driven by practical concerns such as cost, the scale of blocking, the expectations with respect to ease of bypass, and the available technology may also affect the choice of a given filtering approach. Murdoch and Anderson categorize filtering into four types with varying degrees of flexibility and resource requirements: DNS poisoning, IP header filtering, deep packet inspection, and hybrid approaches (see [23]).

In practice, many filtering regimes employ a combination of the above approaches, forming a hybrid filter [9, 11], as used for instance by British Telecom's Cleanfeed system.In the European context DNS filtering based on the CIRCAMP [21] blocklist, which makes use of DNS filtering, is becoming the *de facto* standard, despite the ease by which it can be bypassed. This arguably represents the desire for states to filter quickly and cheaply, without concerns regarding those who may bypass the filter. As we discuss later, this is tacitly acknowledged in the shift in political dialogue from the removal of harmful content, to the prevention of accidental access by innocents. End-user filtering is not included in this analysis.

In the US and Europe, ISPs have traditionally been exempted from liability for the content carried if unaware of potential infringements and if they comply with notifications of take-down. The importance of this principle has been repeatedly underlined by a number of advocacy groups and international organisations [26, 24]. Internet filtering and blocking fundamentally contravenes with this principle by deputising ISPs to effectively intervene in the content carried [4]. By relying on intermediaries to block illegal or undesirable content the administrative and technical burden of filtering, as well as any political backlash, on government can be reduced, whilst providing a new form of crime prevention [21]. This clearly raises serious issues of accountability, due to the lack of public or governmental oversight in the implementation of such methods of control. Arguably the most important concern is transparency of filtering, yet considerations such as overblocking, accountability and oversight are also causes of concern. It is not typically considered acceptable for a filtering agency to publish a list of filtered domains. This is largely due to such lists including direct links to illegal content, and therefore providing an unacceptably valuable resource for those who seek to access such content. How the transparency of such blocklists could be resolved, from a combination of technical and political means, is an interesting open question.

In blocking content the information provided to the user is also a key question. This aspect of filtering can be achieved through *silence*, *error* or *notification*. Silent blocking, as seen in China, provides no overt

notification to a user that their connection has been filtered. As reported by Clayton [6], triggering a filter results in a TCP reset packet being sent to both parties in the connection, although it has also been noted that DNS filtering is also widespread [30].

Error-based blocking presents the user with some form of error when filtered material is encountered. For web access, which makes up the majority of user-focused filtering, HTTP error codes are used by some filtering regimes. These are commonly either a 404 ('file not found') or 403 ('access denied') code, although Microsoft parental controls provide a non-standard 450 ('Blocked by Windows Parental Controls') error message for their own host-based filter. Arguably a 503 ('service unavailable') error would be more meaningful. This approach allows a user some notification that their request has failed but may not provide them with a meaningful way to distinguish between filtered content and simple network errors.

Notification of blocking, as seen in many European filters based on the CIRCAMP list, redirect users to a notification page that informs the user that the content is filtered, and may provide a means through which the user can gain further information or challenge a block. This approach, of those examined here, clearly provides the greatest transparency to the user, although the provision of a technical error code for automatic processing would be desirable at the network level. To discuss these issues on a concrete basis, the next section focuses on the main debates surrounding the attempt to introduce state-mandated internet blocking in France and in Germany.

# 3 Internet blocking debates in France and Germany

France and Germany are liberal democracies with a long-standing commitment to freedom of expression and privacy. However, as in many European countries, freedom of expression is not unlimited but balanced against other principles such as the safeguard of public order or the protection of individuals. Compared with US first amendment protections, the right to free speech in these states is noticeably weaker. In particularly, hate speech regarding race, religion or sexual orientation, as well as denial of the Holocaust and, in France, the Armenian genocide is prohibited. The protection of minors is also a concern for both countries. German and French courts have continually enforced these limitations on freedom of expression, leading to a certain number of internet access restrictions. Both countries have contemplated state-mandated measures to block child abuse images.

The German government first contemplated a self-regulatory filtering system of child abuse images in early 2009. Despite resistance from the internet industry, concerned about their liability and the constitutionality of such a measure, an agreement was signed between the government and five leading ISPs to block online child abuse images on April 22, 2009. The agreement met widespread resistance from ISPs and the left-wing socialist coalition partner, who were concerned about the lack of a legislative basis, as well as experts and citizens, who claimed that the law was a threat to freedom of expression and democracy. An online petition 'no monitoring and blocking of internet pages' (*'Keine Indizierung und Sperrung von Internetseiten'*) reached 50,000 signatures in only four days and became Germany's most successful online petition up to that date, with 134,015 signatures in total. To overcome these criticisms, a legislative proposal was prepared to extend the blocking system to all ISPs and was adopted, as the *Access Impediment Act* (*Zugansgserschwerungsgesetz*, or *ZugErschwG*) on June 18, 2009.

Internet filtering became an electoral issue, most notably for the liberal party that replaced the socialists in the ruling coalition with the conservative ruling party in 2009. The liberals promised to revoke internet blocking, and eventually enacted this through the adoption of a separate law in December 2011. Although the internet blocking law has been formally adopted, therefore, it has never been applied. The government prefers the removal of child abuse material at its source over blocking, a point that has been successfully argued by actors rejecting blocking measures.

On the contrary, in France, opposition to the similar *law on guidelines and programming for the performance of internal security*, commonly referred to as

*LOPPSI 2*, was not successful; the national assembly allowed blocking of access to sites with 'obvious' child pornography, without a court order, in early 2011. This law adds to a growing number of security measures adopted in France since the terrorist attacks of September 2001 that have continually extended the powers of police forces, the amount of surveillance and the strengthening of criminal.

France had previously signed an agreement to block access to child abuse images, racial violence or terrorism in 2008 [10], however concrete internet filtering measures were first discussed in May 2009 when the government introduced them as one part of a wide-ranging law concerned with security and criminality in general. Among the multiplicity of issues raised by the law, internet filtering was not the most controversial. There was widespread critique of criminal sanctions, notably the establishment of a complementary punishment for foreign criminals or the forced evacuation of illegal settlements [17].

In February 2011, a record number of thirteen articles of the bill were ruled unconstitutional [7]. However, the provisions regarding internet filtering were ruled proportionate in terms of balancing public order and freedom of communication. Although the socialist party declared in his presidential program to revoke the LOPPSI 2 bill, it is highly uncertain if this constitutes a priority for the newly elected French president [15].

## 3.1 Methods

The analysis focuses on the debates surrounding the two legislative proposals requiring ISPs to filter online child abuse images in France (*Loppsi 2*) and Germany (*ZugErschwG*). Using Lexis/Nexis, all articles referring to internet filtering measures in the French and German quality press were searched from August 2008 to December 2011. In total, 76 articles from the French quality newspapers *Le Monde*, *Libération* and *Le Figaro* and 270 from the German quality newspapers *Tageszeitung*, *Frankfurter Rundschau*, *Süddeutsche Zeitung*, *Frankfurter Allgemeine Zeitung* and *Die Welt* were relevant. The corpus thus holds articles from left, center as well as right-wing news sources [13, 12].

While it must be acknowledged that much public debate takes place on online platforms such as mailing lists or social media sites, the focus of analysis is limited to quality newspapers that are the main source of information for political decision-makers, hence of greater influence to policy-making [20]. Even in today's highly diverse media environment, the mass media remain important sources for political information [14].

Both the French and the German corpus were coded for statements for or against internet filtering measures. In total, thirteen *frames* were identified for the French articles, sixteen for Germany. Following collective action theory, frames are 'organizing ideas' that are used to simplify and socially construct a given problem and propose solutions and means for achieving these [29, 28]. A frame is an "interpretative schemata that simplifies and condenses the 'world out there' by selectively punctuating and encoding objects, situations, events, experiences, and sequences of actions within one's present or past environment" ([27] p. 137). Frames manifest as demands, proposals, critiques or actions that are not necessarily consciously perceived as belonging to a broader interpretive schemata by the actors expressing them.

The following section presents preliminary findings from this study. Compared to Germany, there was far less debate about internet filtering in France, especially when considering only the print edition of newspapers. Online editions of these publications have been included in the analysis, despite a risk of bias towards the opponents of internet filtering.

## 3.2 Findings

In France, the governing right-wing party was the main proponent of internet blocking measures and found support from the telecommunications industry. Opposition principally stemmed from civil society actors and, to a lesser extent, journalists, the opposition and representatives of the internet industry. In Germany, the main driver of the measures was the conservative Christian-Democrat Party, supported by EU institutions, the police and child protection groups. Digital rights groups were strongly opposed to the measure, and highly vocal about it.

4

They were echoed by all opposition parties, including the liberal party, journalists and parts of the internet industry. References to the need to fight child abuse were made in both cases, by proponents and opponents of the blocking measures and have not been included in the analysis.

The main arguments in both cases referred to principled as well as practical arguments [21]. From the practical side, actors debated whether or not internet blocking is an effective solution for dealing with online child abuse images. Most other arguments related to democratic principles such as the constitutionality and legality of the measure, such as questions of transparency, public oversight, due process, liability, the subsidiarity principle and striking the appropriate balance between different fundamental human rights.

### France

In France, the debate focused on two main arguments: effectiveness and constitutionality or legality of internet blocking. The opponents of internet filtering dominated ten out of thirteen categories, using a wide variety of frames during the debate. They made a total of 168 statements, compared to 92 statements in favour of internet blocking. The opponents' master frame was that internet filtering was not effective to deal with child abuse images. To a lesser extent, they argued that DNS blocking would threaten freedom of expression and generate collateral damage, as well as being unconstitutional. Here, they insisted on the need for prior judicial review, a claim that had dominated the earlier HADOPI debates [2]. Also, opponents repeatedly criticized the proponents of the debates by stating that the government was pursuing a hidden agenda in attempting to introduce a censorship infrastructure and that the Sarkozy government was not to be trusted in any case. They also claimed that blocking would harm civil liberties, especially freedom of expression, and that the blocking would be detrimental to the open architecture of the internet and to net neutrality. Their critique was thus based on a diversity of frames, dominated by practical arguments, with the addition of principled ones.

In contrast, proponents of internet filtering were less visible in general, with fewer claims compared to the opponents of internet filtering. Their arguments referred to three main frames. They clearly dominated the arguments concerning constitutionality and legality, claiming that internet filtering was both legal and constitutional. This was eventually confirmed by the review of the French Constitutional Council, that had been seized by the opposing socialist party, stating that internet blocking of child abuse images was proportionate even without prior judicial review.

Proponents also dominated the frame that internet blocking would protect internet users and prevent crime. They argued that blocking was effective, but received far less visibility than their opponents on this matter. Overall, proponents used a narrow set of frames but dominated the debate on the main principled argument regarding the constitutionality and legality of internet blocking. They hardly engaged at all in discussions concerning the practical side of internet blocking, which was dominated by opponents.

### Germany

In Germany, opponents to filtering successfully occupied both principled and practical arguments, while proponents attempted to emotionalize the debate and opposed one another on the best type of regulation to introduce internet blocking. The debate was dominated by the opponents to internet filtering measures with 814 statements against compared to 678 statements in favour of internet blocking. Compared to the limited number of statements in France, the German debate was far more politicized, with both sides engaging intensively and most categories being heavily disputed.

Opponents argued that internet blocking of child abuse images was not effective, especially through DNS filtering as this could be easily circumvented, and that most exchanges took place through peer-to-peer networks. They also argued that removing the material at the source would be a far more efficient way of dealing with the problem, providing proof that most child abuse material was actually hosted in countries where such content was illegal and police cooperation possible, such as the US or the Netherlands. This would allow for efficient removal through

directly contacting the providers. Opponents also claimed that the proposed measures would lead to a censorship infrastructure detrimental to freedom of speech. All three frames were highly complementary and integrated, and proposed a clear alternative that was referred to by an increasing number of actors.

Proponents argued that internet blocking was an adequate and necessary measure to deal with child abuse images on the internet. This concept includes the repeated attempts by conservative politicians to emotionalize the debate, as manifested by the very controversial projection of child abuse images at a press conference introducing the blocking measures [22]. Leading conservative politicians put forward the argument that all opponents to internet blocking were in fact consumers of child abuse material, but were increasingly criticized for doing so, mainly because the opponents kept pushing for the alternative of takedown over blocking, which established itself as a new master frame of the debate.

Proponents rapidly had to recognize that circumvention of blocks was possible and that blocking would simply 'hinder' access to such material, and not remove it from the internet. This was reflected in the final name given to the law: 'access impediment'.

Proponents also lost on the grounds of the type of regulation that was necessary. The minister for families, supported by the police, initially advocated a 'voluntary' agreement with ISPs that was signed with five major German ISPs on April 22, 2009. However, a self-regulatory regime was contested by all but the christian-democrats and the police, including actors that were not against internet blocking *per se*. These objections focused mainly on ISP concerns over liability, and socialist democrats arguments that legislation was the correct approach.

# 4   Conclusions

In this paper, we have examined the political debate surrounding key European states' attempts to control online information flows. While many countries choose self- or co-regulatory mechanisms to block internet content, others such as France, Germany, Australia and the EU, have attempted to introduce internet blocking through legislation.

State regulation is time intensive and has proven insufficient in effectively regulating global internet traffic. Its main advantage, however, is the opportunity for citizens to debate and question aspects of filtering, in terms of democratic principles such as freedom of expression and the rule of law, and in terms of its effectiveness. The case of Germany demonstrates that internet blocking is not only a highly politicized issue but can also be successfully countered through democratic debate. This is not always the case, as illustrated in France, where internet blocking of child abuse images is legislated and has received the approval of the Constitutional Council.

It is also notable that the question of technical efficacy for filtering was avoided entirely by proponents of filtering in France, while in Germany proponents engaged with this frame but were unable to justify the argument and so forced to backtrack in their claims. Despite this, the technical means of filtering never entered the debate, nor was the choice of DNS filtering as a means to achieve blocking ever questioned. Clearly, both cases would gain from being contrasted with debates (or the absence thereof) in countries opting for self- or co-regulative measures.

Self-regulation and regulation through code have several advantages in dealing with internet issues. Code can more directly and preemptively control human behaviour and allows states to avoid spending administrative and technical resources on doing so, whilst simultaneously avoid a great part of the political fallout from being seen to regulate free speech.

Most worrying, however, is that by displacing the executive choice to filter internet connections from the government to the private sphere, relying on market forces to regulate the type and nature of filtering, serious questions are raised regarding the democratic accountability, legitimacy, and potential for abuse of such an approach. Organized civil society is the most vocal actor in defending civil liberties in the digital realm but are effectively avoided when states deputise ISPs to regulate the internet without a clear legal framework. All stakeholders need to be reminded of the necessity to safeguard democratic principles and rights. If market players are increasingly in charge of

surveillance and filtering online traffic, the need for an independent control mechanism of these systems becomes ever more urgent.

# References

[1] T. Boas. Weaving the authoritarian web: The control of internet use in non-democratic regimes. In J. Zysman and A. Newman, editors, *How revolutionary was the digital revolution? National responses, market transitions, and global technology*, pages 361–378. Stanford University Press, Palo Alto, CA, 2006.

[2] Yana Breindl and François Briatte. Digital network repertoires and the contentious politics of digital copyright in France and the European Union. Paper presented at the "Internet, Politics, Policy: An Impact Assessment" Conference, September 16-17, Oxford Internet Institute, UK, September 16-17 2010.

[3] Ian Brown. Internet filtering - be careful what you ask for. In S.Kirca and L.Hanson, editors, *Freedom and Prejudice: Approaches to Media and Culture*, pages 74–91. Bahcesehir University Press, Istanbul, 2008.

[4] Ian Brown. Internet self-regulation and fundamental rights. *Index on Censorship*, 1:98–106, 2010.

[5] Ian Brown and Christopher Marsden. *Regulating Code: Good Governance and Better Regulation in the Information Age*. The MIT Press, MA, 2013.

[6] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the great firewall of china. In G. Danezis & P. Golle, editor, *Privacy Enhancing Technologies workshop (PET 2006), LNCS*. Springer-Verlag, 2006.

[7] Conseil Constitutionnel. Loi d'orientation et de programmation pour la performance de la sécurité intérieure [loppsi 2] : décision numéro 2011-625 dc. http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/actualites/2011/seance-du-10-mars-2011-[loppsi-2].94818.html, 10 March 2011.

[8] Ronald J. Deibert and Rafal Rohozinski. Beyond denial: Introducing next generation information access controls. In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Information Revolution and Global Politics. The MIT Press, MA, 2010.

[9] Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Denied: The Practice and Policy of Global Internet Filtering*. Information Revolution and Global Politics. The MIT Press, MA, 2008.

[10] Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Information Revolution and Global Politics. The MIT Press, MA, 2010.

[11] Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Information Revolution and Global Politics. The MIT Press, MA, 2010.

[12] C. Eilders. Media as political actors? issue focusing and selective emphasis in the german quality press. *German Politics*, 9(1):181–206, 2000.

[13] François Heinderyckx. *L'Europe des médias*. Editions de Université de Bruxelles, Bruxelles, 1998.

[14] Matthew Hindman. *The Myth of Digital Democracy*. Princeton University Press, 10 2008. ISBN 0691138680.

[15] Raphaële Karayan. Les chantiers numériques qui attendent françois hollande. *L'Express*, 7 May 2012. http://lexpansion.lexpress.fr/high-tech/les-chantiers-numeriques-qui-attendent-francois-hollande_293628.html.

[16] Hans J. Kleinsteuber. The internet between regulation and governance. In OSCE, editor, *The Media Freedom Internet Cookbook*, pages 61–75. OSCE Representative on Freedom of the Media, Vienna, 2004.

[17] Le Monde. Loppsi 2 : le retour de la double peine. *Le Monde*, 22 December 2010. http://www.lemonde.fr/politique/article/2010/12/21/loppsi-2-le-retour-de-la-double-peine_1456443_823448.html.

[18] Lawrence Lessig. *Code: And Other Laws of Cyberspace*. Basic Books, Cambridge, MA, 12 1999.

[19] Maria Löblich and Manuel Wendelin. Ict policy activism on a national level: Ideas, resources and strategies of german civil society in governance processes. *New Media & Society*, 14(3), 2012.

[20] Max McCombs and Donald Shaw. The agenda-setting function of mass media. *Public Opinion Quarterly*, 36(2):176–187, 2010.

[21] T.J. McIntyre. Child abuse images and clean-feeds: Assessing internet blocking systems. In *Research Handbook on Governance of the Internet*. Edward Elgar, Cheltenham, 2012.

[22] Andre Meister. *Zugangserschwerungsgesetz: Eine Policy-Analyse zum Access-Blocking in Deutschland*. PhD thesis, Humboldt Universität zu Berlin, 2011.

[23] Steven J. Murdoch and Ross Anderson. Tools and technology of internet filtering. In Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, *Access Denied: The Practice and Policy of Global Internet Filtering*, Information Revolution and Global Politics, pages 29–56. The MIT Press, MA, 2008.

[24] OECD. Communiqué on principles for internet policy-making. Technical report, OECD, 2011. URL http://www.oecd.org/dataoecd/40/21/48289796.pdf. OECD High Level Meeting On The Internet Economy.

[25] Hector Postigo. Information communication technologies and framing for backfire in the digital rights movement: The case of dmitry skylarov's advanced e-book processor. *Social Science Computer Review*, 28:232–350, 2010.

[26] Frank La Rue. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/hrc/17/27, Human rights Council, 2011. URL http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Human Rights Council Seventeenth session Agenda item 3.

[27] David A. Snow and Robert D. Benford. Master frames and cycles of protest. In *Frontiers in Social Movement Theory*, pages 133–155. Yale University Press, 1992.

[28] David A. Snow, E. Burke Rochford, Steven K. Worden, and Robert D. Benford. Frame alignment processes, micromobilization, and movement participation. *American Sociological Review*, 51(4):464–481, 1986.

[29] Wim B.H. J. van de Donk, Brian D. Loader, Paul G. Nixon, and Dieter Rucht. *Cyberprotest: new media, citizens, and social movements*. Routledge, London, 2004.

[30] Joss Wright, Tulio de Souza, and Ian Brown. Fine-grained censorship mapping – information sources, legality and ethics. In *Proceedings of Freedom of Communications on the Internet Workshop*, 2011.

[31] Jonathan Zittrain and John G. Palfrey. Internet filtering: The politics and mechanisms of control. In Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, *Access Denied: The Practice and Policy of Global Internet Filtering*, Information Revolution and Global Politics, pages 29–56. The MIT Press, MA, 2008.