5 Censors

The debate over control of harmful and illegal material on the public Internet has developed from early discussion in the United States over online obscenity, which led to the Communications Decency Act of 1996. It now spans totalitarian regimes' firewalls, such as China's Golden Shield network blocking system and its 2009 Green Dam project to install filtering software on all new PCs, to democracies' self-regulatory actions, such as the U.K. Cleanfeed-Child Abuse Image Content system and German search engine self-regulation (Marsden 2011).

European nations and U.S. attorneys general (McIntyre 2013) have moved away from a self-regulatory approach toward a coregulatory approach in which ISPs and police cooperate in mandatory filtering of inadvertent viewing (as well as production, consumption, and sale of illegal content), with content blocking widened from child pornography to hate speech to extreme speech (Powell and Hills 2010). The institutionalization of this state-sanctioned and audited approach presents significant new challenges to freedom of expression on the Internet and has led to calls for an Internet bill of rights in the European Parliament, U.S. Congress, and elsewhere (La Rue 2011).

Public Policy and Market Failure

Social Impact of Technology

One requirement driving the Internet's original design was the ability to survive thermonuclear war (Baran 1964; Ziewitz and Brown 2013; Cohen-Almagor 2011). Whether a deliberate design feature or unintended consequence, the Internet's routing system means that data packets can take a wide range of routes from sender to recipient, reducing the ability of

intermediate points to block communications (Clark, Field, and Marr 2010; Kleinrock 2010; Leiner et al. 1998).

This technical detail has had a remarkable impact on the availability of information in developed and emerging economies. While many countries take steps to block access to certain types of content within their own borders (York 2010), censorship is harder to achieve online than with physical newspapers and books and with radio and TV broadcasts. The Internet has enabled much greater worldwide access to news and opinion than any previous medium. However, it has also made it harder for governments to block individual access to content "in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary" (European Convention on Human Rights 1951, sec. 10.2).

Most governments have placed requirements on ISPs and other Internet intermediaries within their own jurisdiction to block access to certain content that is illegal under national laws, by statute and more informal pressure. This almost universally includes child abuse images; incitement to violence, and genocide denial in many countries, particularly in Europe; "glorification" of terrorism; and, in a smaller number of countries, sites encouraging suicide or anorexia. Repressive regimes block a much wider range of sites about controversial issues that might pose a threat to the government (Deibert et al. 2010).

The legitimacy and acceptability of such interventions raise ethical as well as practical questions. Who has the right to judge whether particular content should be shown? When does the intervention amount to inappropriate or unethical censorship?

The EU's approach has been fragmented, partly due to the division of policy responsibility among the three commissioners for the information society, fundamental rights, and home affairs. The last has proposed mandatory blocking of online gambling, child (and adult) pornography, suicide sites, and terrorism supporting Web sites. A leaked January 2011 commission document on online gambling revealed that Domain Name System blocking, the preferred approach, could be used for gambling as well as child pornography blocking (neither approach tackles the source of offend-

ing material, only user access). Civil society group European Digital Rights (2011) reported that "the document explicitly recognises that blocking is 'technically challenging and costly' and that blocking will leave a 'significant' residual level of illegal sites publicly available . . . and that regular updating of a blocking list will be 'costly.'"

The U.S. government is severely constrained by the U.S. Constitution in trying to prevent the publication of almost any type of information. However, administrations such as Richard Nixon's (regarding the leaked Pentagon Papers, a sensitive history of U.S. operations in Vietnam) and George W. Bush's (over the existence of the National Security Agency warrantless wiretapping program) used FBI investigations and legal actions in an attempt to stop the publication of politically sensitive news.

The Obama administration attempted to stop the online distribution of over 250,000 State Department cables allegedly leaked by a U.S. soldier to the WikiLeaks site. WikiLeaks threatens state secrecy or censorship of reporting of its own activities (Benkler 2011a). WikiLeaks collaborated with several European newspapers and the *New York Times* in publishing redacted versions of these cables. They showed the extent of U.S. influence over other countries and, perhaps more pertinent, the graphic accounts from U.S. ambassadors and other senior state officials of the extraordinary levels of corruption in countries as diverse as Saudi Arabia, India, and Kazakhstan. In response, the U.S. government threatened to put the WikiLeaks founder and director, Julian Assange, on trial in the United States and arrested the presumed provider of the cables, U.S. Army soldier Bradley Manning.

As an Australian national, Assange can hardly be described as a traitor to the United States, despite the numerous outraged accusations from congressmen and media commentators. Following the precedent in the Pentagon Papers case (*New York Times Co.* v. *United States* 1971), it is also unclear that Manning would be found guilty of the most serious charge, breaching official secrecy without just cause, under the U.S. Espionage Act 1917.

The assistant secretary of state for public affairs, Philip J. Crowley, resigned in March 2011 after he made remarks in a small seminar at the Massachusetts Institute of Technology about the treatment of Manning in custody: "The exercise of power in today's challenging times and relentless media environment must be prudent and consistent with our laws. . . .

What is happening to Manning is ridiculous, counterproductive and stupid, and I don't know why the [Department of Defense] is doing it" (Smith 2011).

Fundamental Rights

Free speech has been a key part of the U.S. Constitution since the 1791 adoption of the First Amendment, and protected in the 1789 French Déclaration des droits de l'Homme et du Citoyen as "one of the most precious of the rights of man." Article 19 of the Universal Declaration of Human Rights (UDHR) states that:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

This right has been interpreted robustly in relation to online communications. The U.N. special rapporteur on freedom of expression, Frank La Rue, told the U.N. Human Rights Council that the Internet's "unique and transformative nature" enables individuals to exercise a range of human rights and promotes "the progress of society as a whole" (2011, 1). He expressed deep concern that "mechanisms used to regulate and censor information on the Internet are increasingly sophisticated, with multi-layered controls that are often hidden from the public" (9). And he found that "states' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression," since they were not clearly established in law, were for purposes not listed in the International Covenant on Civil and Political Rights, used secret blocking lists, were unnecessary or disproportionate, or lacked review by a judicial or independent body. He also found that imposing liability on ISPs and other intermediaries for illegal content "leads to self-protective and overbroad private censorship, often without transparency and the due process of the law," concluding that "censorship measures should never be delegated to a private entity" and "no one should be held liable for content on the Internet of which they are not the author" (13).

The European Convention on Human Rights and EU Charter of Fundamental Rights protect freedom of expression using very similar language to the UDHR, but Europe's highest courts have heard few cases about government censorship of the Internet. The European Court of Human Rights has shown greater tolerance of laws criminalizing denial of genocide and

incitement to racial hatred than would be expected in the United States, for obvious historical reasons.

In 2003, the Council of Europe drew up an additional protocol to its Cybercrime Convention (ETS no. 189) that requires criminal sanctions for the distribution of "racist and xenophobic materials" (Council of Europe 2003). Its Committee of Ministers has recommended that filtering should generally be left to individual users and national blocking systems "assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society" (2008).

The Assembly of the Council of Europe issued a resolution in 2011 welcoming "the publication, in particular via the WikiLeaks site, of numerous diplomatic reports confirming the truth of the allegations of secret detentions and illegal transfers of detainees published by the Assembly in 2006 and 2007. It is essential that such disclosures are made in such a way as to respect the personal safety of informers, human intelligence sources and secret service personnel" (2011b, sec. 9). The second sentence is presumably in response to the leak and later publication of unredacted U.S. State Department cables in early September 2011.

Repeated U.S. congressional attempts during the 1990s to censor Internet "indecency" were struck down in ringing terms by U.S. courts. The Supreme Court upheld a Philadelphia court ruling that "as the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion. . . . Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects" (*American Civil Liberties Union* v. *Reno* 1997). The furthest the courts have allowed Congress to go is to require libraries and schools receiving specific federal funding to install Internet filters under the Children's Internet Protection Act of 2000.

Iceland's crowd-sourced new national constitution contains robust protection of freedom of expression and the freedom of the media and Internet (Republic of Iceland 2011, Articles 14–16), in response in part to the Icelandic Modern Media Initiative of 2010, proposed by parliamentarian Birgitta Jónsdóttir (Santo 2011). Article 14 states in part: "Censorship and other comparable impediments to the freedom of opinion must never be enacted into law. . . . The access to the Internet and information

Table 5.1
Public policy and market failure

Social impact of technology	Ubiquitous use of broadband gives rise to call for parental controls. Widespread use of blogs and other types of political expression causes state concern leading to censorship. Both have increased since 2000, with users split between those opposed to private censorship mediated by state and others' apparent preference for a walled garden safety environment.
Policy drivers—entry barriers, network and scale effects, competition	Censorship imposes entry costs through technology choice for blocking. Deep packet inspection equipment for traffic monitoring is a dual-use technology, also capable of surveillance and blocking.
Fundamental rights in policy design	Appeal and due process almost entirely lacking. Overall frameworks subject to little democratic scrutiny.
Lessons	Privatization of censorship endemic (even in China coregulation is the claimed model). Greater regional and international transparency standards needed (La Rue 2011).

technology shall not be limited unless by a court verdict and subject to the same conditions as apply to the limits of the expression of opinion." As the youngest parliamentary constitutional standard (albeit with the oldest parliament), it is intended to present a model for a third millennium constitution, as compared with earlier French, U.S., and indeed universal models.

Table 5.1 summarizes these public policy and economic issues. States have increasingly pressured private intermediaries, especially ISPs, to limit access to a wide range of content, from political debate in authoritarian regimes, to gambling sites, to images of child abuse in almost all countries. These controls are often opaque and lacking in due process and democratic scrutiny.

Types of Code Regulation

Electronic Frontier Foundation cofounder John Gilmore famously stated, "The Net interprets censorship as damage and routes around it" (Elmer-DeWitt, Jackson and King 1993).

Many governments have attempted to prevent this rerouting by requiring ISPs to partially block access to foreign Internet sites, or preventing

users from accessing computers connected to the Internet. Examples include proposals by Iran for a "halal" Internet with extremely limited connectivity to other countries, the infamous and leaky "Great Firewall of China," or the Australian single filtered point of international connectivity of the late 1990s (Deibert et al. 2008, 2010).

In 2011, the Egyptian, Libyan, and Syrian governments switched off both Internet and mobile telephony networks in the midst of revolutionary upheaval. A more effective, random, and violent example is the late 1990s Chinese government practice of arresting a random selection of cybercafé users simply for being on the Internet, and interrogating them (Keller 2000).

Assuming that countries choose to allow citizens to use the Internet, there are at least three points of control. The first is self-censorship by the user. This can be in the form of using software filters on end systems to prevent access to most obscene or politically sensitive content, or simply through exercising self-restraint out of habitual fear of state surveillance.

This fear can be less constraining in the Internet environment, where pseudonymity and anonymity are common features and encryption can make traffic extremely difficult to monitor. Recognizing this, many governments both democratic and autocratic have proposed removing such features. These policies are designed to ensure that all users can always be personally identified when using the Internet by such requirements as preregistration and barring access for suspected pseudonymous individuals.

Corporations have carried out the same policies for security or advertising purposes (to prevent spam or ensure more closely targeted advertisements), with the result that many individuals' identities were at risk of disclosure via Facebook to authorities during the Arab Spring in 2011, though rival social network Twitter provided somewhat more robust user identity control (Brown and Korff 2011).

Chapter 7 describes how deep packet inspection can block encrypted connections, permitting only content transmitted "in the clear." Governments can address corporate willingness to control identity by simply making real identity registration a condition of licensing corporations. China has used such conditions to exclude many U.S. corporations, substituting local versions of Skype, social network QQ, search engine Baidu, and other rivals to international applications and services.

Use of real names exposes users to both the risk of political reaction to comments and the prospect of loss of personal data when companies fail to protect that real name registration. South Korea abandoned its policy of requiring user registration linked to national identity number on large Web sites (Index on Censorship 2011) after a data breach exposed 35 million users' personal information (Xinhua 2011b). The leading international human rights bodies issued a joint condemnation of mandatory policies on real names in 2005 (U.N. Special Rapporteur 2005), repeated in 2011 (Akdeniz 2011; La Rue 2011).

The identity of users can also be revealed following court proceedings. U.K. authorities and individuals have been able to secure Twitter, Google, and Facebook account holders' details through what are known as Norwich Pharmacal orders that make these international (California-based) sites codefendants in actions before English courts (Caddick and Tomlinson 2010). U.S. John Doe orders produce similar results.

Beyond users lie ISPs. The user's local ISP will generally operate under license from the national government and can therefore be controlled with some ease. Upstream ISPs can apply filters when accepting traffic from another ISP; for governments that is a particular concern when the handover is an international gateway.

There are various procedures to ensure filtering, all relying on a combination of:

- Upstream labeling (using standards such as the World Wide Web Consortium's now-obselete Platform for Internet Content Selection, PICS) applied by content creators to allow users to apply filters to unwanted content ("blacklisting") or to access only trusted content ("white listing")
- Flagging of potentially harmful sites by users and ISPs, with users of the ISP contacting a hot line (a contact center designed to report and investigate the complaint), with lists of sites maintained by hot lines and police agencies.

In *American Civil Liberties Union* v. *Reno* (1997), the U.S. Supreme Court decided that the virtually unanimous will of Congress to censor the Internet by mandatory filtering was unconstitutionally chilling of speech. *Reno* led directly to the emergence of Internet Content Rating Association (ICRA) in 1999 from PICS and the U.S. Recreational Software Advisory Council system for computer games (Lessig and Resnick 1998; Machill, Hart, and Kaltenhauser 2003). The Communications Decency Act inspired

standards experts to attempt to introduce a wide-ranging labeling scheme for Internet content, the PICS. Resnick and Miller (1996) explain that "the World Wide Web Consortium intended to create a viewpoint-independent content labelling system, and thus to allow individuals to selectively access or block certain content, without government or content provider censorship." As a scheme, its urgency was somewhat reduced by the Supreme Court's *Reno* decision.

The Communications Decency Act was almost immediately replaced by the Child Online Protection Act 1998, which established the Commission on Child Online Protection, whose 2000 report forms the basis for the Family Online Safety Institute's educational approach to child protection from harmful content. The 1998 act was suspended and overturned, and finally the government's last appeal was refused a hearing by the Supreme Court in early 2009. The lack of market adoption of ICRA has been attributed in part to lack of incentives for Web sites unless rating can interoperate with other standards, or more radically unless rating is made mandatory.

Campaign for Democracy and Technology cofounder Daniel Weitzner stated that CDT broadly supported the W3C decision to develop PICS, the Electronic Freedom Foundation was ambivalent, and the ACLU against it, but, he continued, "What was at stake for the industry was their chance to prove they didn't have to be treated like the mass media, and that was the result in the *Reno* decision. . . . The coordination was between the early Internet industry, some part of the civil liberties community and the White House—Gore, Magaziner, Clinton—who gave their blessing right after the *Reno* decision appeared" (Marsden 2011, 114). This was classic industry-led self-regulation that "worked in that it was the right approach, but not as regards interoperability with other incentives for individual website owners."

Co-implementation on child abuse images is clearly not a self-regulatory issue. Where real issues existed, there were some differences between the market-driven U.S. approach ("not self-regulatory but technology will provide the tools") and EU coregulatory standards-based approach toward ICRA. Weitzner concluded, "I don't think there were ever clear expectations set by policymakers as to results, nor were there adequate resources provided for deployment. To my mind that is putting a figleaf on the problem" (Marsden 2011, 114).

Tracking the progress of such labeling standards sheds light on the manner in which technical standards can be used to create content

classification and, ultimately, content standards. At this interface, standards bodies are technical fora with clear influence on content standards, an excellent example of the influence of technology standards on policy.

Filtering and labeling was the obvious tool to ensure that end users had the choice of which content to view without censorship (Berman and Weitzner 1995). It became the default solution to child protection with PICS, an immediate response to the threat of legal classification of indecent content in the United States. It emerged from a meeting organized by the World Wide Wide Consortium in June 1995 to discuss technical solutions for Internet content regulation (Shah and Kesan 2003). Support for the development of Web site quality labels became part of the European Safer Internet Action Plan 1999–2002. Its scheme was taken up, promoted, and adapted by ICRA, and by 2005 it was adapted for use on mobile Internet sites. While support for ICRA included government funding and adoption by some Web sites, most Web sites choose not to label their pages.

In Europe, hot lines were the preferred approach to notify ISPs about potential illegal child pornography (all other illegal content being the responsibility of the notice and takedown regime), with the first hot lines established in 1996. The Internet Watch Foundation hot line had a coregulatory arrangement with police forces in the United Kingdom, though a more formal regulatory arrangement was needed in other countries. The hot lines inspected the material and passed to police for prosecution any material that on scrutiny appeared to be illegal. This case-by-case approach was replaced in 2002 by the removal of entire Usenet groups, leading to broader censorship as it was recognized that some innocent material was bound to be removed.

A blunt approach to blocking Web content is to block all traffic to and from specified Web servers (based on their IP address, or by misdirection of their domain name). Pennsylvania took this approach with a law passed in 2002 (18 Pennsylvania Statutes sec. 7330) that required ISPs to block access to servers within five business days of a notice from the state attorney general.

A district court blocked the enforcement of this law as contrary to the First and Fourteenth Amendments and because it found that orders targeting fewer than 400 sites had resulted in the blocking of nearly 1.2 million innocent sites (*Center for Democracy and Technology* v. *Pappert*, 2004). This occurred because Web servers commonly host more than one Web site—in

one case examined by the court, over 10,000 sites. Similar overblocking problems have been seen with government and court orders blocking sites such as YouTube in India, Pakistan, and Turkey (Deibert et al. 2010).

In 2003, British Telecom (BT), the largest retail and by far the largest wholesale ISP in the United Kingdom, decided as a matter of "corporate social responsibility" to design a more sophisticated system, internally named Cleanfeed, to block its users from accessing overseas child pornography, which had been largely eradicated from the United Kingdom (primary hosting locations then were the United States and Russia). In order to ascertain which specific Web pages and images to block, it used a list of uniform resource locators (URLs) supplied by the industry-funded Internet Watch Foundation, which became known as the Child Abuse Image Content (CAIC) list.

BT's method of dealing with the blocking of specific URLs was a more targeted approach than others adopted by Nordic and Scandinavian ISPs, and discussion ensued in the European Telecommunications Standard Institute about creating a standard for its method of blocking URLs (Marsden 2011). Other ISPs had used DNS blocking, and the CAIC list is harder to circumvent, although users determined to view banned material can use proxy servers and connect to servers using encrypted links or nonstandard ports.

Cleanfeed blocks only what is explicitly blacklisted rather than an entire domain. However, the chaotic result of an attempt to block an image on Wikipedia in early 2009 revealed both the problematic governance and lack of transparency of the CAIC list, the ad hoc nature of Internet Watch Foundation procedures, and the ability of users to reverse-engineer the blocking system (McIntyre 2010; Clayton 2005).

Cleanfeed's success has led others to propose the system be used for purposes other than child pornography, a mission creep that has resulted in European Commission discussion. In the United Kingdom, it was first proposed in 2007 that Cleanfeed/CAIC blocking be made mandatory, then that "extreme" adult pornography be blocked, as well as terrorism-supporting Web sites. In Australia, the proposed national system for mandatory filtering of all hard-core pornography—adult, child, extreme and otherwise—has also been named Cleanfeed (though the plan first made in 2007 was delayed until at least mid-2013 at the conclusion of a convergence of communications review.)

Table 5.2
Types of code and code regulation

Layer	Application or network or both. For example, Chinese ISPs use Golden Shield to filter at entry point to network (and nation), supported by filtering software in client PCs. Western nations typically at network (e.g., Cleanfeed) and filters at client level.
Location	Clients for filters, manufacturers, and ISPs for transport-level filters.
Enforcement of code	National: Egyptian nihilist plug pulling, but negation of code. "Chilling effect" of police enforcement. Golden Shield national solution.

The U.K. government has now persuaded major ISPs to ask new customers whether adult content should be blocked on their own connection (Curtis 2011), and may require that they also ask this question of existing customers. Moreover, Justice Richard Arnold made plain in *Twentieth Century Fox* v. *BT* (2011) that the relatively low cost of using Cleanfeed to block retail customers' access to the Newzbin file-sharing index was what convinced him to impose an injunction, and which is likely to pass muster with the European Court test in *Scarlet Extended* (2011).

We summarize the types of censorship code in table 5.2. This operates mainly at the network layer at users' access ISPs, and at the application layer on users' end-systems in filtering software.

Institutional Political Economy

Kreimer (2006) restated governments' dilemmas in regulating Internet content: "Even where speakers are theoretically subject to sanctions, the exponential increase in the number of speakers with potential access to broad audiences multiplies the challenge for censors seeking to suppress a message" (13). Given the bottleneck control over the user experience provided by ISPs, co- and self-regulatory initiatives populated by these critical actors are central in Internet content regulation (Marsden 2011).

European ISP filtering has emerged from EU-funded labeling and anti-pedophile sexual image reporting hot lines. European funding for hot lines to remove suspected child pornography through reports to the police in each member state continues with multiyear EU funding.

The best-known and oldest example is the U.K. Internet Watch Foundation, but these institutions exist throughout Europe. McIntyre (2010) has considered the U.K. example alongside Ireland, which has a similarly free-standing body. Other European governments have instituted a more formal coregulatory structure with direct reporting to the police. Coordination mechanisms such as the EC Safer Internet Forum play an important role, together with European organizations representing hot lines, national ISP associations, user awareness nodes (Insafe), and ICRA.

Civil society freedom of speech and anticensorship organizations play a role in trying to prevent overzealous censorship. Empirical studies of ISP blocking of content (in the claim of breach of copyright) suggest such a danger is real (Deibert et al. 2010). Conventional labeling and rating methods may not be easily applicable to inappropriate user-generated and posted content.

In 2010 the European Commission proposed a directive that would require EU-wide blocking of sites containing child abuse images. The impact assessment focused wholly on crime and child protection rather than including wider free expression and cost–benefit impacts (Staff Working Document 2009), admitting that Article 21 on blocking access to child pornography on the Internet is not within Council of Europe Convention CETS No. 201, which the remainder of the proposal is meant to fully implement. Blocking proved the main cause of controversy, with critics claiming it to be expensive, pointless, and a diversion from the more effective prosecution of offenders (European Digital Rights 2011).

The proposed directive required that "blocking of access shall be subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers, as far as possible, are informed of the possibility of challenging it." However, such adequate safeguards were not detailed at all, a lacuna in view of state privatization of censorship and known previous inaccuracies and errors in blocking lists. By contrast, European commissioner Viviane Reding (2009) has stated, "We will only be able to reap the full social and economic benefits of a fast moving technological landscape if we manage to safeguard the openness of the Internet" in her speech calling for an EU version of the U.S. Global Online Freedom Act.

After ferocious opposed lobbying by advocates of child protection against digital rights, the European Parliament's Civil Liberties Committee voted by 50 to 0 to remove blocking provisions from the directive (European Digital Rights 2011).

Regulation Using Financial Intermediaries

Commercial application providers, as well as charities that have significant bandwidth costs or rely on Internet-based fundraising, can be effectively censored by regulation of payment or hosting intermediaries. Three somewhat effective examples were targets of U.S. government action: individuals listed in the database of a company that had been used to process payments to commercial providers of child pornography; users of gambling sites based in the small Caribbean island state of Antigua; and readers of the anonymized political source site WikiLeaks. We take these in turn chronologically as the form of censorship in each case became more complex and arguably less successful (as the WikiLeaks material remains available freely even when WikiLeaks itself suffers financial hardship).

In the first case, in 1999, customer details were obtained from a credit card payment processor in the United States, with enforcement taking place in both the United States and Europe (notably the United Kingdom) against several thousand individuals. The identities were clearly available, and payment in itself was represented by police as a motive to commit an illegal action. Several suicides resulted from the publicity stemming from the police operations (McIntyre 2013).

In the second case of offshore gambling, in which a 2006 law banned financial intermediaries from processing payments to or from gambling operators, the case was more complicated for three reasons. First, the underlying activity was illegal only for residents in particular geographies (notably the state of New York, whose attorney general, Eliott Spitzer, was energetically involved in prosecution of the case), but was not illegal in the location where the companies were based. Second, by securing the compliance of the credit card companies, the U.S. government arguably exceeded its jurisdiction in that not all transactions and account holders could be proved to be within the jurisdiction and therefore committing a crime. Third, this activity was shown to be illegal under world trade law, notably in a case before the World Trade Organization (Wu 2007). It was somewhat ironic that the United States should be arguing that several

Chinese government activities against U.S. corporations for engaging in behaviors that are illegal and considered immoral in China should reflect almost exactly the legal arguments that the United States made before the World Trade Organization appellate tribunal (WT/DS285/AB/R 2005). The United States signaled that it was closed for gambling to non-U.S. actors (Wohl 2009).

With the added complication that British citizens have been arrested when in transit through Texas airports for breach of U.S. gambling regulation, it is clear that unlike child abuse images, out-of-jurisdiction gambling sites are much more difficult to regulate. Scott (2007) notes, "The opportunistic arrest of the in-transit chief executive of the UK-based internet gambling company *Betonsports* in Texas in July 2006 is reported to have triggered the company's withdrawal from the US online market and the chief executive's dismissal." This airport transit arrest may remind Internet scholars of the arrest of Felix Somm Munich, the managing director of CompuServe Germany, in 1998, due to his company's failure to block customer access to child pornography (Bender 1999).

Scott (2007) examines case studies of attempts in the United States to prohibit gambling and the U.K. acceptance in the Gambling Act 2006 of the Gibraltar-based offshore status of many key corporate actors. He states: "Achieving compliance with regulatory objectives is challenging enough within domestic regimes where behavioural responses are difficult to predict. But, where that regime involves cross-border business activities, the complex relationships between regulators, businesses and consumers may conspire to frustrate the intentions of the policy makers . . . the near impossibility of preventing determined punters from engaging in internet gaming."

The third case, of WikiLeaks, is even more convoluted. It is not clear that its activities are illegal, whether inside or outside the United States. It is not clear that the U.S. government took any direct action to curtail its activities. It is also uncertain which types of state actions against its founder, Julian Assange, might have been incidental or deliberate attempts to disincentivize the organization from full pursuit of its activities.

The notable elements of the WikiLeaks dispute with the United States and other governments are threefold: U.S. pressure on corporations dealing with WikiLeaks; European governments' legal pressure on Assange and WikiLeaks; and Arab and other countries' reaction to the exposure of

corruption and thus proof of the political danger they faced from the transparency of political processes offered by WikiLeaks and, more broadly, the Internet.

First, the United States apparently put executive pressure on U.S. corporations not to host WikiLeaks servers and successfully obtained information related to the Twitter and e-mail accounts of WikiLeaks sympathizers and presumed collaborators, including an Icelandic member of parliament (Zetter 2011). There was no official communication from the State Department, but politicians such as Senator Joe Lieberman had openly threatened both Assange and the hosting company for his content, Amazon Cloud Services, with retribution for what Lieberman referred to as Assange's "treason." Amazon terminated its WikiLeaks hosting agreement unilaterally, claiming that denial of service attacks on WikiLeaks had created a breach in Amazon's terms of service and that it was ending the contract to protect its other clients.

WikiLeaks relocated its servers to Swedish ISP Bahnhof, with a forty-seven-minute hiatus in service. It responded on Twitter, stating, "If Amazon are so uncomfortable with the First Amendment, they should get out of the business of selling books." Various U.S. financial corporations then stopped cooperating with the WikiLeaks Foundation, among them PayPal, MasterCard, Visa, and Bank of America. U.S. government employees were warned not to view WikiLeaks cables, and the U.S. Air Force computer network blocked the newspaper partners.

The assistant secretary of state for public affairs stated, "We do not control private networks. We have issued no authoritative instructions to people who are not employees of the Department of State" (MacAskill 2010). However, the lack of a direct call to financial and hosting partners of WikiLeaks did not prevent extralegal pressures being applied effectively (Benkler 2011a).

Where direct orders were made by the U.S. government for details of WikiLeaks' linked social media account holders, only Twitter is known to have resisted the executive order, though it was forced to reveal details in March 2011 following a court hearing (Parr 2011). The arguments rejected by the federal judge were presented by those objecting in the case: Icelandic Member of Parliament Birgitta Jonsdottir, Dutch activist Rop Gongrijp, and U.S. security researcher Jacob Appelbaum, together with interveners the Electronic Frontier Foundation and the American Civil Liberties Union.

European authorities reacted to WikiLeaks ambiguously. The Swiss government–owned PostBank suspended Assange's personal account as the conditions for its establishment were fradulently ignored, since he is not a Swiss citizen. In Germany, PayPal refused to accept donations for the Wau Holland Foundation that supported WikiLeaks through donations.

The third governmental reaction to WikiLeaks in censorship terms was that of repressive regimes whose embarrassing secrets were leaked in the confidential cables. These governments broadly censored access to the WikiLeaks site and the various mirror sites that were created after November 28, 2011. Within a week of the first denial-of-service attack on WikiLeaks, there were over a thousand mirror sites in operation. The responses ranged to outright censorship in Zimbabwe and many Arab countries (Black 2010), as well as banning newspapers responsible for the cable releases, effectively a countrywide equivalent of the U.S. government filter.

There were two unexpected results of this blatant censorship, both a symptom of the new political reality of online organization. The first was the Distributed Denial of Service attacks by hacker group Anonymous against the governments of Tunisia and Zimbabwe, as well as various U.S. government sites and financial institutions. The attack took place throughout the two months after the cables were released. The second was the uprisings in Tunisia and Egypt, which had strong censorship but also a strong Internet-literate middle class that had accessed the cables illicitly. Electronic media played a small but significant part in these upheavals.

It is also clear that both text messaging and Internet access were suspected by the Egyptian authorities of being major causes of the earlier revolt in Tunisia, as the Egyptian government chose to shut down mobile networks and Internet access in January 2011, including networks that were majority owned by U.K.-based multinational Vodafone. This was regulation of censorship by private actors: "Companies can find themselves under duress from governments to operate in ways that go beyond legally accountable law enforcement activities" (Global Network Initiative 2011).

Vodafone and others were following direct government censorship orders under the terms of their licenses. The position of mobile ISPs is crucial in this respect, as the number of broadband mobile users has already exceeded fixed broadband users, with a particularly high proportion of mobile users in authoritarian regimes and emerging democracies.

Table 5.3
Institutional political economy

Key actors: national, regional, global	ISPs, international intermediaries, multinational content companies, largely local user groups. Coders multinational (e.g., W3C PICS). Surveillance-industrial complex.
How legitimate and accountable?	Accountability requires transparency to users. Private action subject to little accountability (e.g., put-back provisions). Engineering ethics an undeveloped area.
Multistakeholderism	Little representation for nongovernmental organizations in censorship discussion, with corporate-government discussions largely private. Some discussion apparent (e.g., in hot line governance).
Key technical actor buy-in	ISP-level filtering prevalent since emergence of large-scale spam e-mail problem in early 2000s, continued by BT technical initiative. Need for standards and best practices to ensure minimal collateral damage from blocking, particularly where technology sold to totalitarian regimes' ISPs.
Lessons	Private censorship accompanied by government encouragement, sponsorship (e.g., hot lines). Democracies increasingly need political control of export of technology conducive to repression.

Table 5.3 summarizes this institutional political economy. The key actors are technical and financial intermediaries, law enforcement agencies, and content producers. Civil society groups have played a limited role, although child protection groups have been a high-profile voice for restrictions on child abuse images.

Outcomes

Technologies of censorship can be used for commercial and political control. Deibert et al. identify four phases of regulation, from openness prior to 2000 to denial of access and to control (2008, 2010). This chapter has described the critical decisions made in 1996 and 1997, with the decision to allow ISP liability to be limited. Prior to that, Internet development was a legal mess, if a code success.

The developments since 1997 have been toward increasing commercialization led by advertising revenues (notably with the development of Yahoo! and Google search and the Facebook social network site), yet direct

censorship has been relatively limited, governments apparently largely favoring indirect controls through ISPs and these new intermediaries. The failure of the PICS initiative through ICRA was an unfortunate illustration of the limits of self-regulation when free riding was not disincentivized. Its success would have required much greater levels of participation by Web site operators, who had little incentive to do so.

Government attempts to substantially increase the levels of online censorship have largely taken place by encouraging private ISPs to limit access to suspect material for their own customers. Where there is no direct contractual relationship between ISP and content provider, no explicit possibility to enforce regulation applies, and the ISP is responsible for content only when it has been given notice of its potential harmful or illegal nature. At that point, it may take down such content prior to investigating the complaint: notice and takedown (NTD) under the Electronic Commerce Directive (ECD) and, for copyright-infringing material, the DMCA. ISPs that act as "mere conduits" (Article 12, ECD) have no liability if they follow such rules, nor do content hosting services, subject to some exceptions (Article 14, ECD).

Such regimes have been criticized as a "shoot first, ask questions later" approach in which ISPs have little incentive to investigate the complaints of alleged pornographic, defamatory, or copyright-infringing content (to name the three most common categories for NTD). The role, effectiveness, and impact on ISP competitiveness of filtering is also essential to the roles of NTD regimes under ECD. The suggestion that other interlocutors, notably search engines and P2P systems, provide alternative routes for users to share potentially illegal or harmful content, raises the issue of the reform or amendment of the ECD to embrace these categories of content intermediaries.

The real fork in the road in the past ten years has arguably been the development of large-scale filtering technologies, which provided for some measure of national—through access ISP—jurisdiction. Thus, the landmark *UEJF et LICRA* v. *Yahoo!* case of 2000 in France established filtering by IP address and the beginning of national jurisdiction outside the United States (Reidenberg 2002). Filtering software imposed by government appears to have run into both practical and financial difficulties, with the Australian mandatory filter delayed by government (Australian Associated

Press 2010) and Chinese attempts to impose mandatory filtering by July 2009 also abandoned in favor of a public institution filter for schools and cybercafés. The latter Green Dam technology prospects are uncertain (BBC 2010).

In 2012, Twitter and Blogger, widely lauded for their promotion of free expression, announced they had introduced systems that allowed content to be blocked in specific jurisdictions after requests from national authorities. This was claimed to be preferable to content being blocked globally (York 2012).

More broadly, the Internet as used by political dissidents has been subjected to government demands on intermediaries. Governments required access to e-mail and social media accounts in order to censor content, as well as Web site takedown. There is a crisis in corporate governance for multinational information intermediaries including:

- ISPs such as BT
- Mobile ISPs such as Vodafone
- Equipment manufacturers such as Cisco
- Collecting societies such as Société d'Auteurs Belge
- Search engines from Yahoo! to Google (Marsden 2008; Deibert et al. 2010).

Yahoo! suffered a crisis of confidence in regulation in both its failure to convince French courts that it could identify national users in the *UEJF et LICRA* v. *Yahoo!* case and its six-year failed court battle to persuade California courts to prevent standing of the French judgment in California (Reidenberg 2005). More dramatically Yahoo! handed over dissident records to Chinese police in 2001, resulting in the ten-year imprisonment for political dissidence of Wang Xiaoning and others (Goldsmith and Wu 2006).

As a result, companies sought guidance on their activities in countries with differing human rights approaches, whether in Europe, where racist extremism and genocide denial are offenses, or in China, where free speech faces severe obstacles. Viviane Reding discussed whether European law should ban European information technology companies from activities in repressive regimes and concluded that it was unnecessary. A year later, the European Parliament (2010) condemned Nokia Siemens Networks, a gigantic European multinational telecoms and Internet company, which

had sold monitoring center control equipment to Iran, where it was used to control mobile text messages in the protests after the 2009 presidential election there.

Attempts have been made continually by U.S. Congressman Chris Smith to introduce a global online freedom act (H.R. 3605 [2011]) "to prevent United States businesses from cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance, to fulfill the responsibility of the United States Government to promote freedom of expression on the Internet, to restore public confidence in the integrity of United States businesses, and for other purposes." This is intended to prevent the activities of such companies as Yahoo! in China and Lucent Alcatel or Cisco in China and the Arab world. It has failed to reach a full House vote, as was the case with its predecessors in 2009 and 2007 (111th Congress: H.R. 2271 and 109th Congress: H.R. 4780). The European effort of 2009 also failed in Parliament.

Where legislation failed, so also has private U.S. court action under the Alien Tort Statute of 1789, which permits action against U.S. companies for damages incurred as a result of their collaboration with repressive foreign governments, intended originally for collaboration with the former colonial power. Hu Kunming (2007) reports that Yahoo! settled with dissidents and their families on November 13, 2007, in part to avoid further poor publicity in the United States after Congressional Foreign Affairs Committee inquiries into their collaboration, and that of Microsoft and other U.S. multinationals, with Chinese censors. Yahoo! also agreed to establish a fund to assist dissidents placed in such circumstances in the future. In 2010, Google finally withdrew from China after various censorship incidents and highly suspicious hacking of activists' Gmail accounts. In 2011, Cisco was sued by several activists under the Alien Tort Statute for its activities in providing filtering allegedly specifically marketed as efficient in finding banned Falun Gong images (Sui-Wee Lee 2011), but the actions have made little progress.

Censorship of political dissidence is not confined to noted repressive regimes. In late 2011 it was reported that South Korea's state censors were removing 10,000 Web sites a month accused of various immoral and dissident purposes such as nebulous claims of preventing social harmony, including that of the independent academic member of the "standards commission." South Korea in 2007 had required all users of popular Web

sites (those with readership of more than 100,000 users a day) to register their real names in order to comment, but announced in 2011 that it would abandon this policy after the massive CyWorld data breach that lost the personal data of the majority of the population (Xinhua 2011b). This is not to be overly sanguine about Internet censorship, but to realistically assess its success in avoiding the extremes of censorship evident elsewhere in the more traditional media.

The pseudonymity and anonymity of the Internet, together with user encryption, means that determined and skilled users can generally avoid detection when avoiding censorship. However, the collaboration of Western multinationals with repressive governments puts ordinary users at risk. While human rights declarations, corporate responsibility charters, and proposals for legislation are welcome, and the undermining of the more reactionary elements of state censorship in pursuit of consenting adults continues, the direction of censorship appears to be toward greater attempts to control users, even as the number of users, and thus difficulty in mass censorship, is rising.

Secretary Clinton's (2010, 2011) confused but clarion call for some types of Internet freedom establishes in international statecraft that foreign sovereign censorship is for most purposes discouraged by the United States. Communications, and digital technology in part, has played a significant role in political change such as the Arab Spring of 2011. However, caution needs to be exercised, as both the Middle East and North Africa and earlier democratic movements owe much more to university education, economic changes wrought by globalization, and the incompetence of rulers than they do to Twitter, Facebook, or text messages. (Recall that the overthrow of the European Communist regimes was achieved in 1989–1990 without modern digital technology.)

Nevertheless, a combination of the Internet, mobile networks, and satellite television, including, notably, Al-Jazeera has fashioned the latest claim of digital technologies of freedom following de Sola Pool (1983). If the railways, telegraphs, intercontinental private shipping, and electricity created incredible social and economic changes in the nineteenth century, with attendant political uprisings (Spar 2001), so the Internet appears to be creating its own vortexes and currents in the international political economy (Marsden 2004).

Private censorship is barely discussed in 2011 Clintonian doctrine, except as a result of direct government action, such as that exerted on Vodafone's Egyptian operations (Arthur 2011a). She condones a coregulatory type of censorship, for example, that exerted against Amazon's cloud computing hosting in the face of furious political pressure. This followed the WikiLeaks exposé of U.S. condoning of many dozens of murderous tyrants worldwide in full knowledge of the scale of their corruption, torture, and other abuses of suffering populations. Notably, she insisted that the United States has taken no direct extralegal action against WikiLeaks, which is correct only in the narrowest sense (Ingram 2011). Therefore, types of private censorship for political advantage or pecuniary gain are condoned by the Clinton doctrine.

In response to Secretary Clinton's criticism, China has made a great play of its adherence to the UDHR and has published a white paper on its citizens' freedom to use the Internet: "Chinese citizens fully enjoy freedom of speech on the Internet. The Constitution of the People's Republic of China confers on Chinese citizens the right to free speech. . . . Vigorous online ideas exchange is a major characteristic of China's Internet development, and the huge quantity of BBS posts and blog articles is far beyond that of any other country" (People's Republic of China 2010, sec. III).

Kingma (2008) argues that the tendency toward re-regulatory policy extends beyond child protection into online gambling, among other areas, where it is felt that risk regulation has overliberalized controls on gambling markets (Mikler 2008). In as contested and complex an environment as online child protection or gambling, where realistic solutions involve a great deal of interference and state regulatory control over individual behavior, it is unsurprising that the types of legitimacy and effectiveness that have long been the norm offline have been abandoned in favor of stylistic and superficial calls for self-regulation, in the knowledge that the problems are insoluble. The EU has varying standards of gambling regulation, ranging from very liberal laws in, for instance, the United Kingdom to more onerous regulations and even prohibitions against offshore gambling in Sweden and Italy. There is an impasse in the EU regarding the regulation of gambling (Hornle 2010; European Digital Rights 2011).

Table 5.4
Outcomes and divergences

Transparency	Blocking lists private, obscure reasons for removal, no generic reporting duty on ISPs.
Enforcement	More consistent put-back would help to make enforcement fairer. Private censorship removes user rights. General classes of content censored (e.g., Usenet). Blind alley as bad guys can always access. Enforcers should go to source: arrest producers.
Interoperability	Cleanfeed better approach compared to DNS blocking collateral damage. Iran's "halal Internet" worst of all possible worlds, with not even interconnection.
Efficiency	Blocked illegal content remains partially accessible. Significant costs imposed on intermediaries.

We summarize these outcomes in table 5.4. Even in democratic states, the operation of blocking systems is often opaque and a disproportionate interference with freedom of expression.

Gambling, WikiLeaks, and political repression may be smoking guns for censorship, but ubiquitous traffic management policies may encourage deployment of technologies that permit discrimination at far more subtle levels, using deep packet inspection, than these crude examples (Peracchio 2011). We turn to this subject in chapter 7.