International Journal of Communication 11(2017), 4583–4609 1932-8036/20170005

The Inconsistent Work of Web Filters: Mapping Information Access in Alabama Public Schools and Libraries

CHRIS PETERSON[1]
MIT Media Lab, USA

SHANNON M. OLTMANN
University of Kentucky, USA

EMILY J. M. KNOX
University of Illinois Urbana–Champaign, USA

Recent popular and academic discussions regarding the Internet have raised the question of whether and how networked intermediaries have a (dis)integrating social effects. In this study, we use public records of configurations of Internet filters in Alabama public schools and libraries to show how different institutions implement nominally consistent content standards inconsistently. We argue that these varying implementations are both significant and troubling for two reasons: first, they overreach the stated goals of the legislation with which they in principle comply; second, they may contribute to a broader epistemic breakdown by fragmenting the kind of information made available through and across public institutions.

Keywords: Internet filtering, filter bubble, censorship, critical infrastructure studies, algorithms, categories, CIPA, libraries, schools, Leigh Star

Chris Peterson: petey@mit.edu
Shannon M. Oltmann: shannon.oltmann@uky.edu
Emily J. M. Knox: knox@illinois.edu
Date submitted: 2017–01–22

[1] The authors would like to thank Shawn Musgrave, formerly of MuckRock, who helped coordinate the public records requests that produced the bulk of our data set; Professors Nick Seaver and Ed Schiappa, who provided helpful feedback on earlier drafts; our anonymous reviewers, whose constructive criticism significantly sharpened and strengthened this article during revision; and interlocutors at the *Theorizing the Web* (2016) and *Partnership for Progress on the Digital Divide* (2017) conferences, as well as colleagues at the Center for Civic Media, where initial findings were shared and early arguments made.

Sorting the Internet to Filter It: Breitbart Is "Society," But Jezebel "Adult"

In January 2017, during the Trump presidential transition, radref, an electronic mailing list for librarians, began discussing a surprising filtering phenomenon. Some members had noticed that Lightspeed, an Internet filtering provider commonly used by public libraries, categorized *Breitbart*, the right-wing tabloid formerly edited by Trump advisor Steve Bannon, as "Society.Politics,"[2] while classifying *Jezebel*, the feminist blog, as "Adult."[3] Meanwhile, others observed that the filtering system Websense classified *InfoWars*, published by noted conspiracy theorist Alex Jones, as "News and Media," while classifying *Buzzfeed*, which publishes both news and media, as "Entertainment." As the librarians compared notes on their filtering systems, they encountered other idiosyncratic classifications, with often surprising implications for the kind of information made (un)available to their patrons through their institutions.[4]

In this example, we see the convergence of two different senses in which the Internet is metaphorically "filtered." The metaphor of Internet "filters" has historically described "technical blockages to the free flow of information across the Internet that [actors] put in place or require others to institute" (Zittrain & Palfrey, 2008, p. 2). In another, more recent sense, the metaphor of "filters" (Pariser, 2011) has been used to describe algorithmic personalization, especially on social media, that curates and presents different information about the world to different users, which may undermine democratic solidarity and consensus (Sunstein, 2009).

In this article, we bring these two ideas together in the context of contemporary Internet filtering in Alabama public schools and libraries. We compare public records of Internet filtering configurations to demonstrate that filtering regimes are implemented inconsistently between institutions nominally governed by the same content standards. We identify three sources of this inconsistency, arising from strategies used by administrators to tailor global filtering systems to local preferences. We find these filtering regimes (a) overreach the stated goals of the legislation with which they in principle comply and (b) may also contribute to a broader epistemic breakdown by fragmenting the kind of information made available through and across public institutions. We conclude by discussing future research directions to better understand the lived experience of administrators and patrons who design, deploy, use, and resist Internet filtering in public institutions.

Design and Execution of This Study

This study draws on data gathered as part of a larger research project that seeks to discover and associate incidents of censorship in public institutions with everyday geopolitical entities, such as states, municipalities, and districts, and thus metaphorically "map" the terrain of information made available

[2] https://archive.lightspeedsystems.com/SubmitDomain.php?Domain=breitbart.com.

[3] https://archive.lightspeedsystems.com/SubmitDomain.php?Domain=jezebel.com.

[4] E-mail on file with authors.

through these institutions in these locations.[5] Our primary source materials are public records obtained from schools and libraries, which, we believe, provide a different, and complementary, perspective from which to survey this territory compared to more conventional methods, such as surveys and news reports.

We have previously published an article discussing the history and methodology of using state public records laws for research purposes (Oltmann, Knox, Peterson, & Musgrave, 2015). Although public records laws are frequently invoked by journalists and activists to uncover source material for their stories and campaigns, the use of public records requests in scholarly work is less common. Some recent exceptions include the work of Charles Davis, a journalism professor who has used public records requests to report on local censorship trends (O'Connor, 2012), and Amy Johnson, an anthropologist who sued the CIA for failing to turn over records related to the management of its Twitter account as part of her research on Twitter and global politics (Annear 2017; Johnson, 2017).

Some benefits of our approach include the ability to compel the collection of comprehensive records from public institutions. For example, other well-known data sets of censorship incidents are typically maintained by professional advocacy organizations, such as the American Library Association (ALA), and sourced by local teachers and librarians who report incidents of patron or parent requests for reconsideration of materials. These data sets often form the basis of news coverage and organizational decision making. However, they typically exclude curatorial decisions made by professionals or configurations of technical systems, as well as requests that, for whatever reason, are not reported to the organization. In principle, requests for public records under compulsion of law should source more/different data.

Some challenges to this approach include a lack of robust compliance or, conversely, a deluge of data too voluminous to analyze easily. Responses may depend on whether institutions have the resources, expertise, and risk tolerance to fully respond to a request. Public records cannot capture what goes unrecorded in the ephemeral life of institutions; nor, depending on response rates and patterns, are they necessarily "representative" of some general phenomenon. However, public records requests can provide primary source materials for study and may point the way toward future research opportunities by making visible documentary traces of controversies that can be subsequently studied in richer detail.

For this study, we used federal databases from the Institute of Museum and Library Services (IMLS) and the National Coalition of Education Statistics (NCES) to build a data set of 351 public institutions—134 public school districts and 217 public library systems—in the state of Alabama.[6] This data set, which used data gathered in 2011 and published in 2013, included names and addresses of the institutions; we added e-mail addresses based on information posted to institutional websites and other public sources. We chose to target districts and systems (as opposed to schools and branches) because a

[5] More information can be found at the project website (http://mappinginfoaccess.org).

[6] For public school districts, we used the Common Core of Data Local Education Agency (School District) Universe Survey (FY2013) conducted by the National Coalition for Education Statistics. For library systems, we used the Public Libraries Survey (FY2013) conducted by the Institute for Museum and Library Services.

precursor project in Massachusetts showed that public records requests sent to branches were often escalated to senior administrators for response (Peterson, 2013). We chose Alabama as the first site for this project because it is alphabetically first among the 50 states. It is worth noting for this study that Alabama has a relatively weak open records law, with no specified time frame for response or penalties for noncompliance (Oltmann et al., 2015; Oltmann, Peterson, & Knox, 2017). Because this is the first test of our approach, it is hard to know whether and how the weakness of the legal compulsion affected our study. In the broader project, for which we are currently pursuing funding, we intend to apply our approach across the remaining states and to include such comparisons as both considerations and findings.

Pursuant to the aforementioned Alabaman open records law (Alabama Open Meetings Act, 2005), we drafted a letter[7] requesting public records related to censorship. For the purposes of this article, this request asked for the following:

- Any records related to Internet filtering, including but not limited to
    - any current acceptable use policies, Web publishing policies, or equivalents;
    - any current contracts with Internet filtering services and/or providers;
    - any current categories of content that their provider offers to block, along with which categories their institution currently blocks; and
    - any modifications to the standard configuration of their filter, including lists of sites, services, URLs, keywords, or other identifiers that have been specifically configured as forbidden or allowed (i.e., blacklists/whitelists)

In January 2014, we mailed a paper copy of the request to each of the 351 institutions and also delivered electronic copies via MuckRock, a citizen journalism service news site that helps individuals file, track, and organize public records requests. Our requests, as well as all subsequent exchanges and responsive documents, are publicly available on the MuckRock website.[8] We also asked professional communities of school and library administrators to circulate notices explaining our study to relevant electronic mailing lists in an attempt to assuage anxieties and increase responses. We ceased to seek new responses from institutions in November 2014.

At the end of our study, we had received full or partial responses from 222 institutions (138 libraries, 84 schools), which were read and coded by responsiveness to request(s) by one of our authors. Of these, 107 (71 libraries, 36 schools) acknowledged filtering the Web and identified their filtering software, and 40 (23 libraries, 17 schools) sent records of Internet filtering configurations. Eight public libraries said they did not filter the Internet; no public school made the same claim. Responsive institutions reported using 28 different filtering software systems. Among them, there is no apparent

[7] A draft of the letter we sent is published at our project website.

[8] All requests and responses are published at https://www.muckrock.com/accounts/profile/GeoCen/

standard configuration, or even a standard configuration of standards: we received text files, spreadsheets of links, screenshots of websites, faxes of printouts of screenshots of websites, and other multimodal responses.

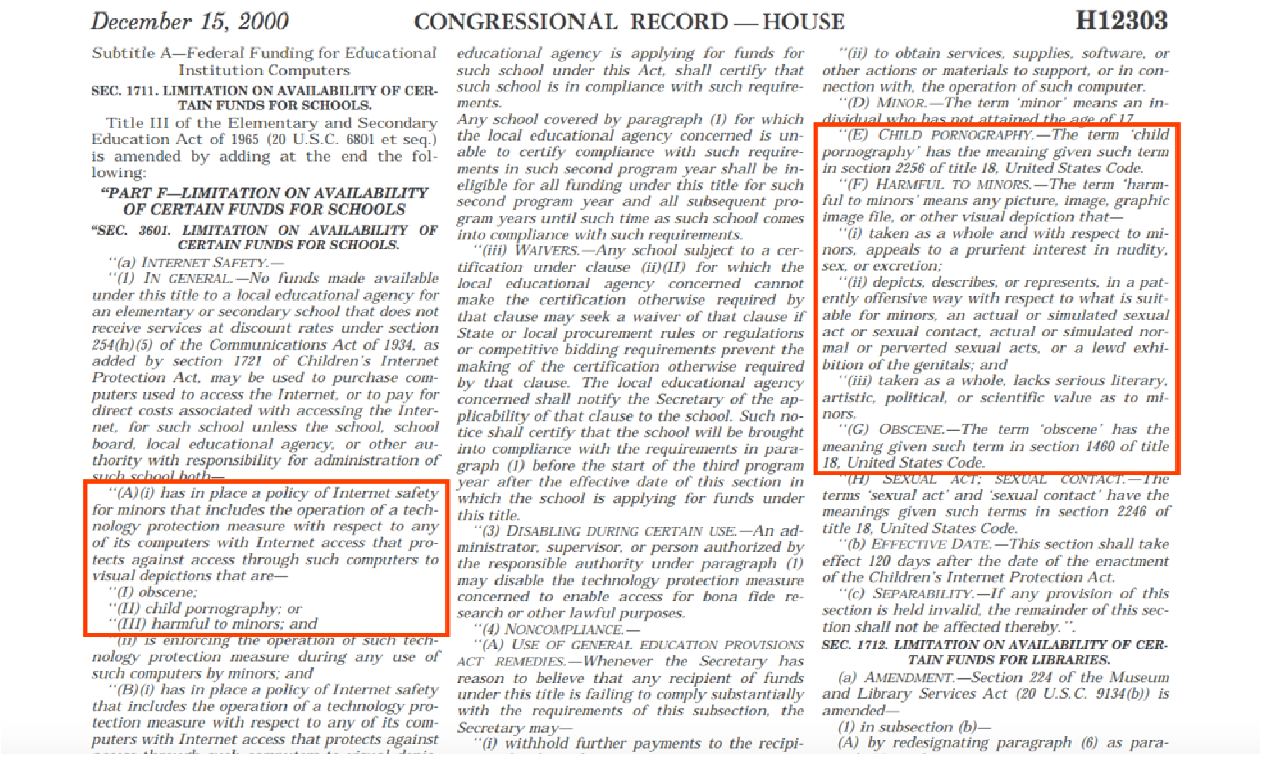
Overview of Internet Filtering in American Public Schools and Libraries

In 2000, after years of pressure from child-protection groups (Minow, 1997), the United States Congress passed the Children's Internet Protection Act, or CIPA,which required American public schools and libraries seeking federal funding to implement a "technology protection measure" (TPM), defined as a "technology that blocks or filters Internet access to visual depictions that" fall into the specified categories of obscenity, child pornography, or being harmful to minors (Children's Internet Protection Act, 2000). However, the text of CIPA offers no guidance for how stakeholders ought to evaluate if a visual depiction qualifies as obscene or harmful to minors, or how any disputes over such decisions might be redressed and resolved.[9] It does not specify what features a TPM (or, interchangeably for the purposes of this article, an Internet filter) should have, or how such features ought to be configured (see Figure 1).

Instead, CIPA delegates these decisions to local authorities (e.g., school administrators and library directors) who were (and are) free to select, configure, and implement a filter to meet their needs (Minow, 2004). Anticipating objections on First Amendment grounds, Congress also prescribed that an administrator at a complying institution "may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose" (CIPA, 2000).

Nonetheless, CIPA was immediately challenged by a coalition, led by the American Library Association, that argued the bill imposed an unconstitutional condition on public institutions to block access to constitutionally protected speech. In 2003, the Supreme Court upheld CIPA in an unusual plurality decision with several concurring opinions (*United States v. American Library Assn., Inc*., 2003). While each opinion applied different reasoning to reach a shared conclusion, all agreed that the interest in protecting minors from harmful content was compelling, and that the provision to disable filters for adult patrons rendered the objection moot. Since 2003, all public schools and most public libraries have implemented technology protection measures as prescribed by CIPA (Caldwell-Stone, 2013).

[9] In fact, even the internal definitions referenced within CIPA are often mistaken or circular, sometimes in revealing ways. For example, although the text of the bill cites Section 1460 of Title 18 of the United States Code for the meaning of "obscenity," this section does *not* define the term *obscene* but instead specifies the punishment for those apprehended possessing obscene materials with intent to sell on federal property. Section 1461, immediately following, *does* define material that is "nonmailable" on account of being obscene or crime-inciting; of the six paragraphs enumerating nonmailable materials, five of them describe information about how to obtain or perform an abortion.



December 15, 2000 CONGRESSIONAL RECORD — HOUSE H12303

Subtitle A—Federal Funding for Educational Institution Computers

SEC. 1711. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.

Title III of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 6801 et seq.) is amended by adding at the end the following:

"PART F—LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS

"SEC. 3601. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.

"(a) INTERNET SAFETY.—

"(1) IN GENERAL.—No funds made available under this title to a local educational agency for an elementary or secondary school that does not receive services at discount rates under section 254(h)(5) of the Communications Act of 1934, as added by section 1721 of Children's Internet Protection Act, may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such school unless the school, school board, local educational agency, or other authority with responsibility for administration of such school both—

"(A)(i) has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—

"(I) obscene;

"(II) child pornography; or

"(III) harmful to minors; and

"(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors; and

"(B)(i) has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against

educational agency is applying for funds for such school under this Act, shall certify that such school is in compliance with such requirements.

Any school covered by paragraph (1) for which the local educational agency concerned is unable to certify compliance with such requirements in such second program year shall be ineligible for all funding under this title for such second program year and all subsequent program years until such time as such school comes into compliance with such requirements.

"(iii) WAIVERS.—Any school subject to a certification under clause (ii)(II) for which the local educational agency concerned cannot make the certification otherwise required by that clause may seek a waiver of that clause if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by that clause. The local educational agency concerned shall notify the Secretary of the applicability of that clause to the school. Such notice shall certify that the school will be brought into compliance with the requirements in paragraph (1) before the start of the third program year after the effective date of this section in which the school is applying for funds under this title.

"(3) DISABLING DURING CERTAIN USE.—An administrator, supervisor, or person authorized by the responsible authority under paragraph (1) may disable the technology protection measure concerned to enable access for bona fide research or other lawful purposes.

"(4) NONCOMPLIANCE.—

"(A) USE OF GENERAL EDUCATION PROVISIONS ACT REMEDIES.—Whenever the Secretary has reason to believe that any recipient of funds under this title is failing to comply substantially with the requirements of this subsection, the Secretary may—

"(i) withhold further payments to the recipi-

"(ii) to obtain services, supplies, software, or other actions or materials to support, or in connection with, the operation of such computer.

"(D) MINOR.—The term 'minor' means an individual who has not attained the age of 17.

"(E) CHILD PORNOGRAPHY.—The term 'child pornography' has the meaning given such term in section 2256 of title 18, United States Code.

"(F) HARMFUL TO MINORS.—The term 'harmful to minors' means any picture, image, graphic image file, or other visual depiction that—

"(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

"(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

"(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

"(G) OBSCENE.—The term 'obscene' has the meaning given such term in section 1460 of title 18, United States Code.

"(H) SEXUAL ACT; SEXUAL CONTACT.—The terms 'sexual act' and 'sexual contact' have the meanings given such terms in section 2246 of title 18, United States Code.

"(b) EFFECTIVE DATE.—This section shall take effect 120 days after the date of the enactment of the Children's Internet Protection Act.

"(c) SEPARABILITY.—If any provision of this section is held invalid, the remainder of this section shall not be affected thereby.".

SEC. 1712. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR LIBRARIES.

(a) AMENDMENT.—Section 224 of the Museum and Library Services Act (20 U.S.C. 9134(b)) is amended—

(1) in subsection (b)—

(A) by redesignating paragraph (6) as para-

Figure 1. Scan from the Congressional Record of CIPA, with relevant sections outlined.

As J. C. Bertot and his collaborators have shown in regular surveys conducted over the past two decades, public institutions, especially libraries, continue to play a major role in providing/mediating access to the Internet to ordinary people; indeed, "building digitally inclusive communities has become one of the key functions of public libraries in the United States as well as in many other nations" (Bertot, Real, & Jaeger, 2016, p. 271). As a result, "any misconceptions about personal computers or broadband being in virtually all Americans' homes are quickly dispelled when considering the level of demand that is currently placed on public libraries' technological infrastructure" (Bertot et al., 2016, p. 277). A 2014 ALA policy briefing reported 60 million Americans lacked either a home broadband connection or smartphone, and that they disproportionately belonged to socioeconomically disadvantaged groups (Batch, 2014). As such, the constraints and consequences of Internet filtering (a) affect many people and (b) especially impact the poor, elderly, and less-educated individuals who are less likely to have home broadband.

These trends hold true for our (arbitrarily) selected field site of Alabama. According to the IMLS, the 138 libraries in our study reported 4.3 million public Internet computer uses per year; according to the American Community Survey, the population of the entire state of Alabama is 4.8 million. According to the 2013 Digital Inclusion Survey conducted by Bertot and colleagues, 25% of Alabama libraries reported that patrons experience a wait time for public access computers (Bertot et al., 2014), which demonstrates the level of demand for institutional Internet access; the 2014 Digital Inclusion Survey showed that rates and kinds of Internet usage in Alabama libraries were broadly consistent with national averages (Bertot, Real, Lee, McDermott, & Jaeger, 2015).

Prior academic studies of CIPA-compliant Internet filtering, published mostly in the library and information science literature, have, among others, conducted adoption-rate surveys (Comer, 2006), analyzed differences in adoption between schools and libraries (Jaeger & Yan, 2009), reviewed the impact of filtering on the role of the library as a public Internet access point (Jaeger, Bertot, McClure, & Langa, 2006), and studied student behavior in filtered and unfiltered school environments (Yan, 2009). Some have attempted to quantify "error rates" of blocking, typically by creating a list of links that the authors decided should, or should not, be blocked, and running those links through the filter to see which were or were not blocked (Resnick, Hansen, & Richardson, 2004). However, we were unable to find any studies of the specific kinds or configurations of filters implemented across different institutions, and thus how access to the same information might vary between them.

Meanwhile, the advocacy and jurisprudence regarding Internet filtering, as described above, has historically figured the controversy as between proponents of free expression and guardians of moral propriety (Caldwell-Stone, 2013). After the passage of CIPA, some scholars and advocates introduced the issue of student intellectual development and agency as a consideration for policy makers (Yan, 2009). Some baseline unpredictability of filtering behavior in libraries had been observed even before Congress enacted CIPA (Minow, 1997), and a recent policy briefing by the ALA identified "overbroad" filtering as both a trend among and a challenge for libraries (Batch, 2014). However, the informational, which is to say political, consequences of inconsistent filtering in public institutions have been largely overlooked in the academic and professional literature.

Our work builds on and expands this prior work by studying how specific TPMs are actually implemented. By doing so, we intend to (a) empirically demonstrate idiosyncratic classification practices that create inconsistent access to information across public institutions, despite nominal standardization by CIPA, and (b) link this specific inconsistency in public institutions to a general inconsistency, and resulting fragmentation, ascribed to contemporary information intermediaries.

Conceptual Framework and Analytical Approach

Although most studies of filters and filtering have treated TPMs as universal objects that are either implemented or not, we instead consider TPMs as disunified objects, with local configurations, that are implemented differently at every site. This tactic of "localizing the global" (Latour, 2005) helps us trace the strategies and tactics by which software systems, in cooperation with their designers and users,

bring a "hidden order" (Geiger, 2011) to the chaos of the Internet. Our study thus works to complicate simple binaries, such as filtered/unfiltered, connected/disconnected, and censored/uncensored, into a more robust understanding of an Internet that appears and operates differently depending on where any given user is situated, both socially and geographically, and how they are mediated by local technologies and institutions.

For this article, we reviewed the filtering configurations and contracts of the 40 institutions that submitted responsive records. The previously-described multimodal character of these records made them difficult not only to compare but also to share in a conventional academic article: responses included screenshots of configuration panels, lengthy printouts of lists of links, and spreadsheets representing the output of a database access control list, not all of which are equally amenable to the same methods of analysis nor representation in a publication.

Because we received so many types of records, from so many different institutions, in the sections below we selected a subset of records that are typical of those received (in both content and pattern) and relatively easily reproduced in an academic article. Primarily, these are screenshots of filtering configurations or lists of links that can be compared against each other to reveal continuities and discontinuities. This basic technique is common across disciplines (such as history and media studies) that rely on material artifacts to supplement their textual analysis; we were especially influenced by the fragmentary documentation used by Latour (1999) and Mol (2002) in their respective studies of transit systems and the human body, where scraps of records reflexively foreground the uncertainty, contingency, and precariousness of the study itself. We have also assigned each respondent a pseudonym to mask their institutional identity.[10] The complete data set of records is published and available for review at the MuckRock website.

Because the core focus of this article is the specific implementation of filters across different institutions and any (in)consistencies that result, we have organized our findings as three distinct strategies that emerged as patterns in the records. These sociotechnical strategies are not necessarily distinct and indeed often overlap. The benefit of this approach is that it makes it easier to see, from the perspective of a local administrator (i.e., the agent implementing the configuration and producing the record), how their TPM organizes the Internet into something that can be filtered, how they can tailor their TPM to their goals, and how different types of TPMs locate the filtering agency in different places. The result of this approach is to both illustrate and emphasize the widespread inconsistency in implementation that we found.

Strategies to Organize and Filter the Internet

[10] Pseudonyms were assigned based on the canonical cast of characters drawn from Bruce Schneier's (1996) "Applied Cryptography." We did not promise this to our respondents as a precondition. Instead, it is a decision we have made after the fact to help shield those who, potentially against their immediate interests, responded to our request. The deanonymized results are available on the MuckRock site and with the authors.

Strategy A: Categorizing the Kinds of Content to Filter

As discussed in the overview of filtering in American public institutions, CIPA prescribes a category model of content to block. The law requires that TPMs block content categorized as obscenity, child pornography, or being harmful to minors, while offering no guidance on determining how content should be classified into those categories or how disputes over classification should be resolved. As such, TPMs are often designed around categories (including, but not limited to, those specified by CIPA) that local administrators can allow or block.

"Assigning things . . . to categories is a ubiquitous part of work in the modern, bureaucratic state," Bowker and Star (1999, p. 284) observed. The design and deployment of categories in filtering systems can be understood as an example of what Adele Clarke (2016) calls "anticipation work." , Clarke, working in Star's tradition, defines anticipation work as the processes and practices by which complex reality is simplified into usable components of systems. Anticipation work happens both before and during the design of a system, but always with an eye toward making future tasks more manageable. Categories can thus help make visible the most salient organizing concepts and immediate goals of software designers and users.

Consider, for example, the category schema designed and deployed by K9 Web Protection, one of the most common filtering solutions used by our respondents. Seventeen of our respondents indicated that they use K9, and four of them provided legible configurations. K9 is a product of Blue Coat Systems, a network security company acquired by Symantec in June 2016 for $4.65 billion. Free for home use, user licenses are available to schools and provided to libraries by the state of Alabama through the state system.[11]

K9 offers users five preconfigured selections tuned to different levels of permissiveness, ranging from "high" (protects against all default-level categories plus social interaction and unrated sites) to "monitor" (allows all categories—only logs traffic). Users who wish to customize their configuration may select from 24 "commonly blocked categories," as well as 47 "other categories" for a total of 71 kinds of content that might be worth filtering. Yet none of these categories cleave to the classification framework prescribed by CIPA. Instead, they instantiate a different ontological (and moral) order, operating around and across that contemplated by Congress to anticipate the additional needs of filtering institutions (Batch, 2014).

[11] According to one of our respondents, a director at a small public library, K9 is "is provided to us free of charge through the state library system," and is used to "block all pornography sites, sites with sexually suggestive keywords or content, sites that contain hate based materials, sites that promote terrorism, and some gambling sites" (see 2014-03-11T10/51/03.522365 Communication.txt, on file with the authors).

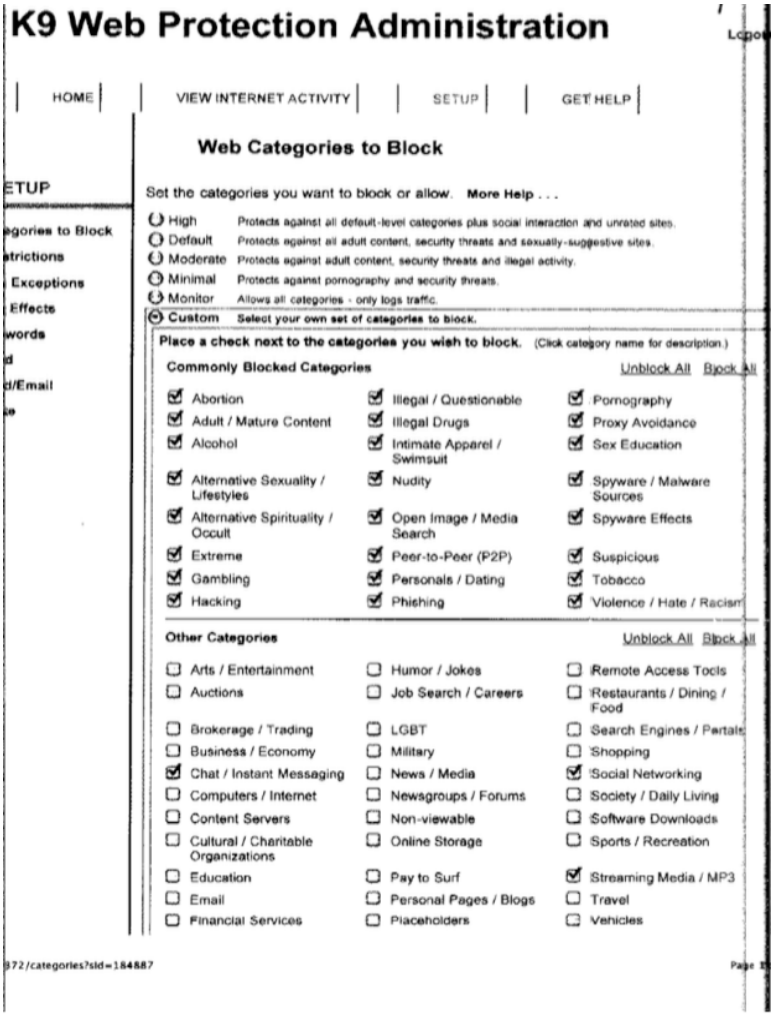


Figure 2. K9 Configuration at Alice Municipal Library.

Figure 2 records the configuration of the municipal library in a small town (pop. ~1,500) in northeastern Alabama that serves ~3,500 computer users annually. It has a single, part-time librarian who has implemented a custom configuration of K9 that blocks *all* 24 "commonly blocked categories"—including Alternative Sexuality/Lifestyles, Sex Education, and Suspicious—as well as four Other Categories including Games and Social Networking.

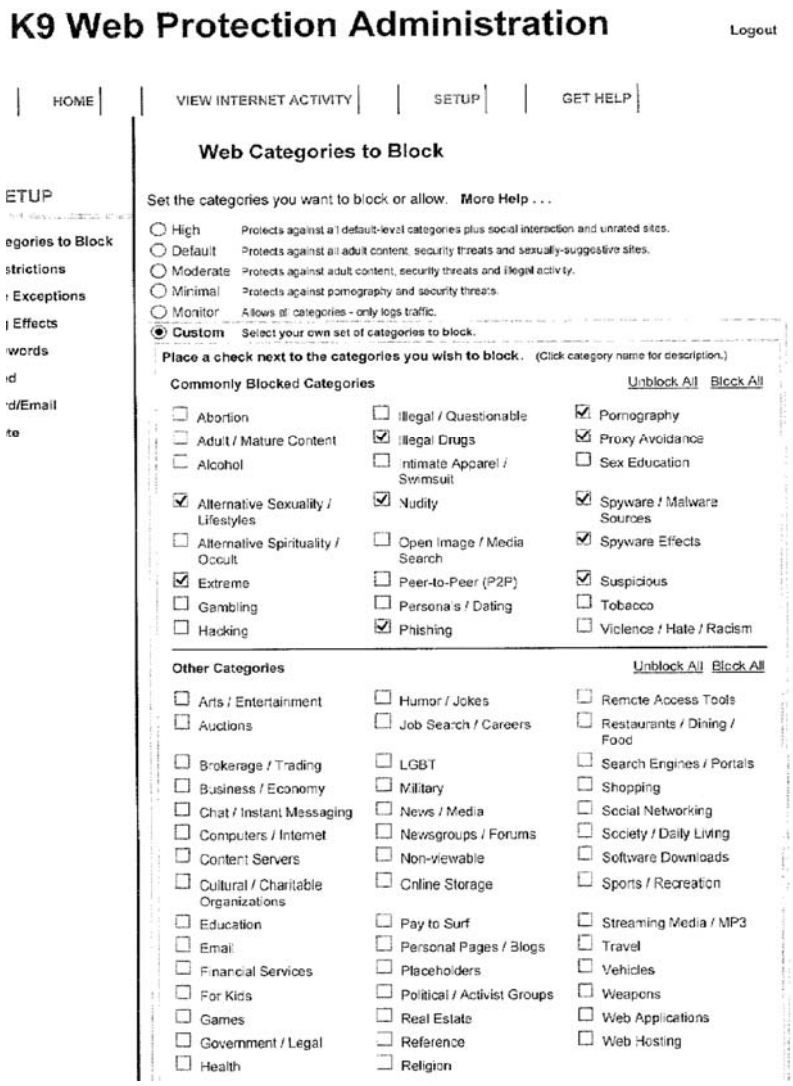


Figure 3. K9 Configuration at Bob County Library.

By comparison, consider the configuration of K9 in Figure 3, implemented by a county library located in a county seat (pop. ~15,700) in midwestern Alabama that serves ~6,200 computer users annually with a staff of two. It has also implemented a custom configuration of K9, but this one blocks only 10 "commonly blocked categories" and none of the "other" categories. And although the library blocks Alternative Sexuality/Lifestyles, Intimate Apparel and Adult Content remain unchecked.

In these cases, the categorization scheme is the same, but the categories selected are different. Despite operating in similar contexts, serving similar constituents, and using the same software, these two libraries have implemented very different filtering regimes and thus offer their patrons access to Internet content that is meaningfully and intentionally different according to the software designed to filter it. The discrepancy invites further research as to why these decisions were made. Why are there different content standards for similar constituencies? And why, at both institutions, is blocking queer content (described with the euphemism of "alternative sexuality") a higher priority than conventionally prurient material?

Differences in categorization schemes produce another axis of inconsistency, which we can see by comparing K9's categories to those anticipated by OpenDNS, another popular filtering company and subsidiary of networking giant Cisco. Its primary filtering product, known as Umbrella, is specifically targeted at the K–12 educational market, and invokes CIPA compliance in its advertising, which also claims a client base of 40,000 schools. Six of our respondents rely on OpenDNS for filtering.

Like K9, OpenDNS offers a range of preconfigured options. As can be seen in Figure 4 (below), it offers three instead of five, with its "high" setting calibrated to exclude "all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters." Similarly, it provides 59 categories, foregoing K9's "Extreme" but adding "German Youth Protection," possibly to assist international clients using OpenDNS to comply with the German equivalent of CIPA.

Figure 4. OpenDNS Configuration at Carol Municipal Library.

Figure 4 records the custom OpenDNS configuration of a library located in a small town (pop. ~2,600) in southeastern Alabama that serves ~7,900 computer users annually. Note the partial overlap with the other two municipal libraries we have already seen, and the marked difference in kinds of content imagined to exist between the two systems. Again, despite a nominal compliance with a standard law, and a generally similar community of constituents, the kind of information made available through this intermediary again deviates not only from the standards of CIPA but from the practice of nearby institutions.

The variance between category scheme and selection seen in these three examples is typical of the 30 category configurations we received: In our records, no two implementations of the same system had the same selection of common categories, and no two filtering systems had the same category set. Indeed, different filtering products often compete on the differences in number, kind, and comprehensiveness of categories. Barracuda Networks, a publicly traded network security company used by three of our respondents, offers a "Web Security Gateway [that] includes a preinstalled URL list containing millions of URLs classified into 95 categories for easy and efficient content filtering" (Barry, 2015). Similarly, Trustwave, a cybersecurity subsidiary of Singaporean multinational telecommunications conglomerate Singtel, promises to "[filter] millions of Web sites in 100+ categories—without impacting bandwidth or productivity" (Trustwave, 2014, p. 1).

As such, while most filtering systems offer standard categories, the categories are not standardized: Indeed, differences between systems produce a perceived comparative advantage in the market as filtering companies contend for clients. If every software system offered the same categories, populated by the same websites and operating with the same rules, filtering providers would have fewer things to compete upon. The inconsistency thus arises from both sides of the implementation: at the point of design by the software company to produce a differentiated product, and at the point of configuration by the administrator to meet their local preferences. To adapt the old software aphorism to the logic of the market, the inconsistency of categories across filtering systems is not a bug, but a feature.

Strategy B: Lists That Forbid or Permit

Sometimes, however, features fail, and infrastructures do not work as expected, becoming suddenly visible upon breakdown (Star, 1999, p. 382). In the case of filtering, this most commonly happens when a site that should be accessible is not, or conversely, when something that should be blocked is not. These edge cases are a signal that the categories (meaning in this case both the conceptual schema and the mechanisms that populate them) are overly exclusive or inclusive.

In these cases, software systems, like other infrastructures, are held together with what Star called "articulation work" (Star, 1999, p. 385). Articulation work refers to the process of naming (and taming) the "monsters" (Haraway, 1992) that resist the naturalization of categories (Bowker & Star, 1999, p. 310). As Gerson and Star (1986) put it, "articulation is [necessary] because the definition of adequate provision shifts according to local circumstances . . . [systems] must be aligned or tailored to a set of implementation conditions that cannot be fully specified ahead of time" (p. 258). The (often invisible) work of articulation can be found by "looking for these processes in the traces left behind by coders, designers, and users of systems" (Star, 1999, p. 385).

In the case of filtering systems, articulation is often accomplished by lists: blacklists (links or expressions that are always blocked) and whitelists (links or expressions that are always permitted) that override the standard scheme and selection of categories. By allowing/enacting adjustments around the edges of categories, these lists "[package] a compromise . . . that closes the system locally and temporarily so that work can go on" (Gerson & Star, 1986, p. 266). In a filtering system, lists of links and

other expression are thus both form and function: durable inscriptions that simultaneously record and perform the work of articulation (Johnson, 1988).

For example, consider Figure 5, a (partial) record of the blacklist implemented by a public school district in a Birmingham suburb.

At first glance, this list resembles what the media scholar Ian Bogost, in his study of the philosophical function of lists, describes as "a pile of incoherent crap spilled at the foot of the reader" (Bogost, 2012, p. 41). Upon closer inspection, however, some patterns emerge: The IP addresses ending in /GALLERY/, /RANDOM/, and /NEXT/ are (or were) all part of the Wordle text-cloud platform; the hubristic CANTBLOCK.ME is a proxy server for routing around school filters; Facebook, Snapchat, and Gmail require little explanation in the context of schools cracking down on peer communication. However, the rationale behind other decisions is harder to infer, such as the decision to blacklist WestEgg.com, the personal website of Manhattanite Morgan Friedman, who describes himself as "a language-loving polyglot [who is] good at getting people really excited about things." ("Steven Morgan Friedman, n.d., p. 2).

All Allow:

HTTP://74.125.65.104/TALK/
HTTP://74.125.65.105/TALK/
HTTP://74.125.65.106/TALK/
HTTP://74.125.65.147/TALK/
HTTP://74.125.65.99/TALK/
HTTP://74.125.65.103/TALK/
HTTP://CAMPSILOS.ORG/EXCURSIONS/
HTTP://128.121.225.2/EXCURSIONS/
HTTP://WWW.CAMPSILOS.ORG/EXCURSIONS/
HTTP://74.125.65.120/IMAGES/
HTTP://74.125.45.120/IMAGES/
HTTP://VIDEO.NYTIMES.COM/
HTTP://199.239.137.36/
HTTP://WWW.VIDEO.NYTIMES.COM/
HTTP://THE911MEMORIAL.MAGNIFY.NET/
HTTP://208.70.246.59/
HTTP://WWW.THE911MEMORIAL.MAGNIFY.NET/
HTTP://SCHOOLTUBE.COM/
HTTP://216.146.46.10/
HTTP://216.146.46.11/
HTTP://WWW.SCHOOLTUBE.COM/
HTTP://50.56.54.61/
HTTP://2001:4801:1063:1F5:5:BCAD:0:0/
HTTP://WEBMAIL.CLOUDOPSCENTER.NET/
HTTP://208.70.246.24/
HTTP://MEXCONNECT.COM/
HTTP://WWW.EVERNOTE.COM/SHARD/
HTTP://204.154.94.81/SHARD/
HTTP://EVERNOTE.COM/SHARD/
HTTP://CONNECT.FACEBOOK.NET/EN_US/ALL.JS/
HTTP://WWW.CONNECT.FACEBOOK.NET/EN_US/ALL.JS/
HTTP://MASHABLE.COM/
HTTP://98.129.174.16/
HTTP://WWW.MASHABLE.COM/
HTTP://PINTEREST.COM/
HTTP://107.20.237.30/
HTTP://184.73.231.199/
HTTP://WWW.PINTEREST.COM/
HTTP://TWIMG.COM/
HTTP://210.163.219.24/
HTTP://WWW.TWIMG.COM/
HTTP://T.CO/
HTTP://199.59.148.12/
HTTP://WWW.T.CO/
HTTP://EARTH.GOOGLE.COM/
HTTP://74.125.45.101/
HTTP://74.125.45.102/
HTTP://74.125.45.113/

Figure 5. Configuration of David City Schools blacklist.

All Block:

HTTP://CANTBLOCK.ME/
HTTP://74.63.84.190/
HTTP://WWW.CANTBLOCK.ME/
HTTP://WWW.WORDLE.NET/GALLERY/
HTTP://74.125.113.121/GALLERY/
HTTP://WORDLE.NET/GALLERY/
HTTP://216.239.32.21/GALLERY/
HTTP://216.239.34.21/GALLERY/
HTTP://216.239.36.21/GALLERY/
HTTP://216.239.38.21/GALLERY/
HTTP://WWW.WORDLE.NET/RANDOM/
HTTP://74.125.113.121/RANDOM/
HTTP://WORDLE.NET/RANDOM/
HTTP://216.239.36.21/RANDOM/
HTTP://216.239.38.21/RANDOM/
HTTP://216.239.32.21/RANDOM/
HTTP://216.239.34.21/RANDOM/
HTTP://WWW.WORDLE.NET/NEXT/
HTTP://74.125.113.121/NEXT/
HTTP://WORDLE.NET/NEXT/
HTTP://216.239.36.21/NEXT/
HTTP://216.239.38.21/NEXT/
HTTP://216.239.32.21/NEXT/
HTTP://216.239.34.21/NEXT/
HTTP://WWW.6LYRICS.COM/
HTTP://174.142.192.14/
HTTP://6LYRICS.COM/
HTTP://FACEBOOK.COM/
HTTPS://69.171.229.11/
HTTPS://69.171.242.11/
HTTPS://66.220.147.33/
HTTPS://69.171.229.13/
HTTPS://WWW.GMAIL.COM/
HTTPS://74.125.65.19/
HTTPS://74.125.65.83/
HTTPS://74.125.65.17/
HTTPS://74.125.65.18/
HTTPS://GMAIL.COM/
HTTPS://74.125.159.17/
HTTPS://74.125.159.18/
HTTPS://74.125.159.19/
HTTPS://74.125.159.83/
HTTP://WWW.WESTEGG.COM/
HTTP://74.208.10.131/
HTTP://WESTEGG.COM/
HTTPS://74.125.47.83/
HTTPS://74.125.47.17/
HTTPS://74.125.47.18/
HTTPS://74.125.47.19/
HTTPS://74.125.45.17/
HTTPS://74.125.45.18/
HTTPS://74.125.45.19/
HTTPS://74.125.45.83/
HTTPS://31.13.77.55/
HTTP://SNAPCHAT.COM/
HTTP://64.202.189.170/

Figure 6. Configuration of David City Schools whitelist.

Meanwhile, the (partial) whitelist from the same school shows the mirror image of sites that local administrators inscribed to specifically permit (see Figure 6). The whitelist is several pages longer than the blacklist, suggesting that the filtering software blocks more things that need to be accessed than the other way around. Jostled together we find *The New York Times*, Mashable, and *MexConnect*, "an electronic magazine devoted to providing quality information about Mexico, and promoting Mexico to the world" ("All About *MexConnect*," n.d., p. 1).

In the previous section, we demonstrated inconsistencies in the design and selection of the anticipatory work performed by categories. In the case of the articulation work performed by lists, we see inconsistencies not only across institutions but even within institutions. The administrators of David City Schools block Gmail and Snapchat but permit Pinterest and Twitter and have added Facebook to both the

blacklist and the whitelist. The inconsistencies made apparent by these lists invite further inquiry into the local controversies and decisions made by institutional administrators.

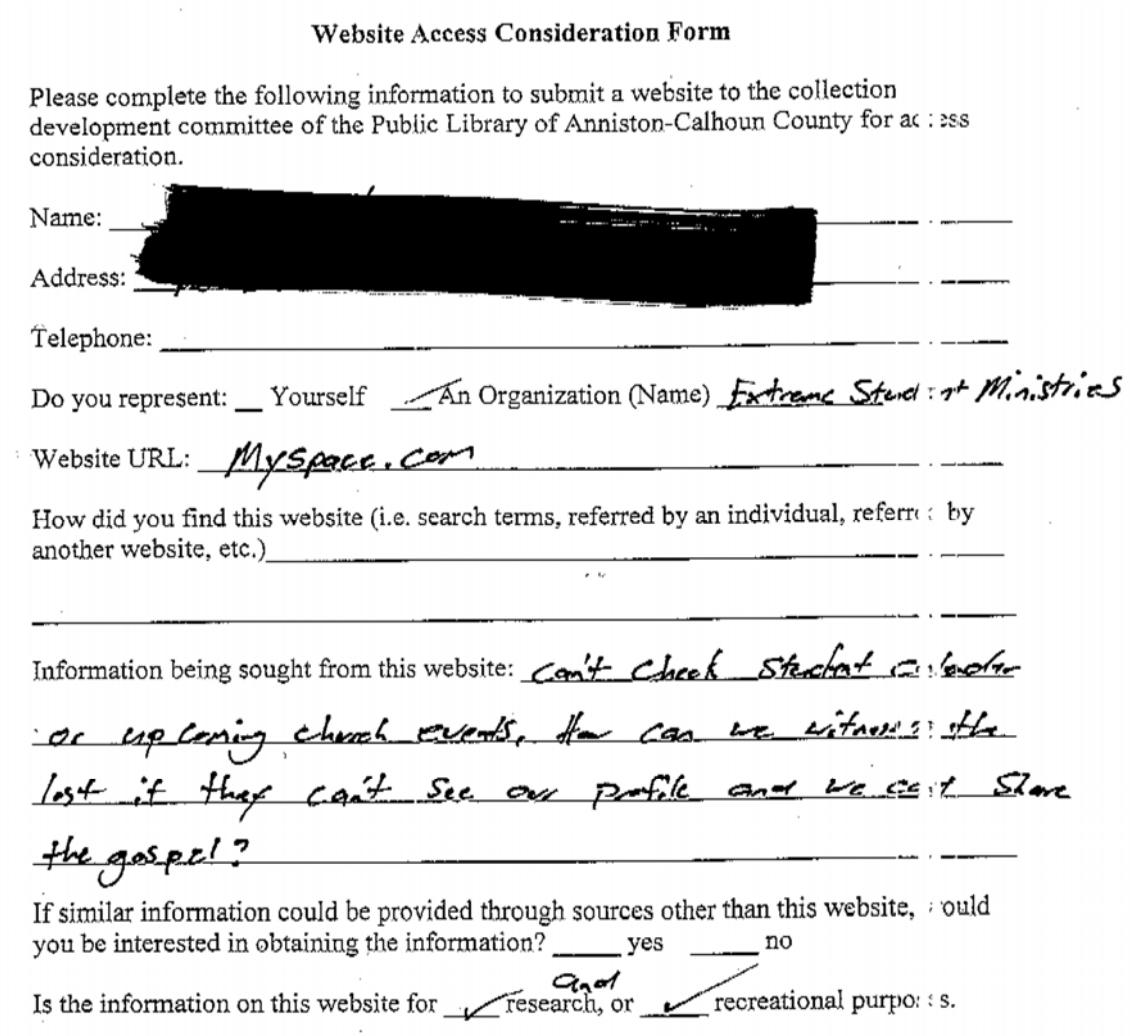
Strategy C: Mixing Agencies—Public and Private; Algorithms and Engineers

In "The Ethnography of Infrastructure," Star (1999) quotes the anthropologist Gregory Bateson to observe that infrastructures are properly understood/studied as "a relationship or an infinite regress of relationships" (Bateson, as cited in Star, 1999, p. 379). Star deploys this epigram to introduce a discussion of some methodological challenges to studying infrastructures. The sprawl of infrastructure across time, space, and kinds of actors—where studying an irrigation system involves understanding the work of piping, policies, and plumbers alike—means that, as Ananny and Crawford (2016) argue,

> rather than privileging a type of accountability that needs to look *inside* systems, that we instead hold systems accountable by looking *across* them—seeing them as sociotechnical systems that do not *contain* complexity but *enact* complexity by connecting to and intertwining with assemblages of humans and non-humans. (p. 2, emphasis in original)

The complex sprawl of filtering systems, which include general categories and local lists, classifying algorithms and configuring administrators, provides responsive parties with the flexibility to distribute authority, credit, or blame to other agents entangled in the assemblage. In our study, we found this complexity enacted as such in a third strategy deployed by our respondents to tailor filtering systems to local needs. Unlike Strategies A and B, this strategy does not arise from our respondents' skilled use of technological features built into the filtering system but rather from the complexity of the system itself, as respondents appeal to the many and different kinds of actors entangled in a filtering system when they justify their implementation.

Sometimes, these appeals take the form of emergent alliances, where an actor enrolls other actors, both humans and nonhuman, into alliances to make and defend certain arguments (Latour, 2005). Consider, for example, the request shown in Figure 7, received in 2006 by a public library in northeastern Alabama, by an adult patron asking the library to unblock Myspace for (in the language of both CIPA and the Supreme Court) a bona fide lawful purpose.



Website Access Consideration Form

Please complete the following information to submit a website to the collection development committee of the Public Library of Anniston-Calhoun County for access consideration.

Name: [redacted]

Address: [redacted]

Telephone: [redacted]

Do you represent: __ Yourself ✓ An Organization (Name) Extreme Student Ministries

Website URL: MySpace.com

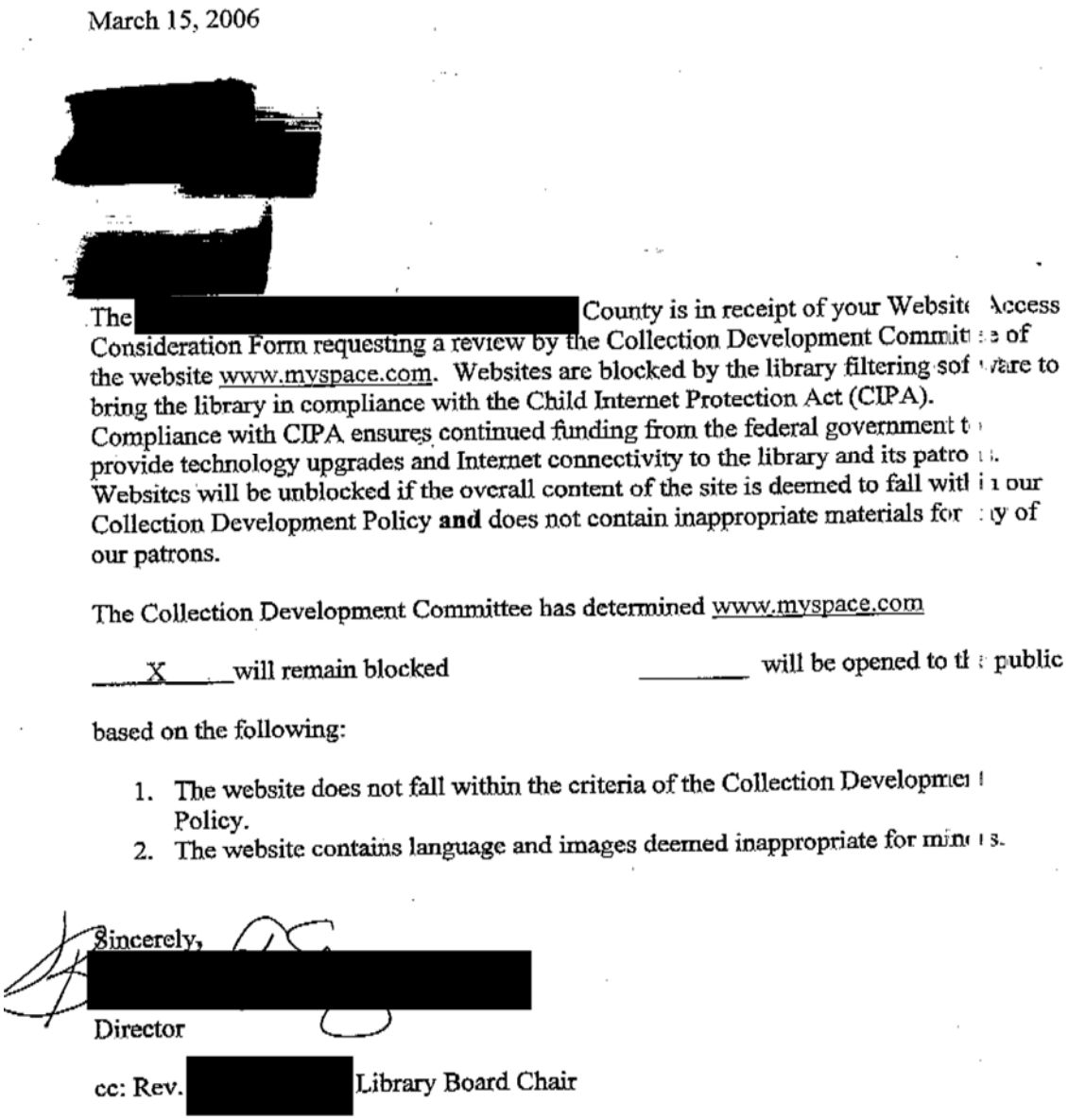
How did you find this website (i.e. search terms, referred by an individual, referred by another website, etc.) [redacted]

Information being sought from this website: can't check Stephat calendar or upcoming church events. How can we witness the lost if they can't see our profile and we can't share the gospel?

If similar information could be provided through sources other than this website, would you be interested in obtaining the information? ____ yes ____ no

Is the information on this website for ✓ research, and ✓ recreational purposes.

Figure 7. Request from a patron to unblock Myspace.



March 15, 2006

[redacted]

The [redacted] County is in receipt of your Website Access Consideration Form requesting a review by the Collection Development Committee of the website www.myspace.com. Websites are blocked by the library filtering software to bring the library in compliance with the Child Internet Protection Act (CIPA). Compliance with CIPA ensures continued funding from the federal government to provide technology upgrades and Internet connectivity to the library and its patrons. Websites will be unblocked if the overall content of the site is deemed to fall within our Collection Development Policy **and** does not contain inappropriate materials for any of our patrons.

The Collection Development Committee has determined www.myspace.com

___X___ will remain blocked _____ will be opened to the public

based on the following:

1. The website does not fall within the criteria of the Collection Development Policy.
2. The website contains language and images deemed inappropriate for minors.

Sincerely,

[redacted]

Director

cc: Rev. [redacted] Library Board Chair

Figure 8. Response to patron's request to unblock Myspace.

In this case the patron, writing on behalf of the organization Extreme Student Ministries, complains that without access to Myspace, which serves as the organizing platform and event calendar for local Bible studies, they will be unable to "share the gospel." In response, the library's director, cc'ing its ordained board chair, refuses to unblock Myspace, and justifies this decision by appealing to both CIPA

and their collection development policy (see Figure 8). The library director thus enrolls ministers, federal legislation, and local policy in an unlikely alliance to defend its filtering regime against evangelicals and Myspace, and in contradiction to the Supreme Court's requirement that legitimate content be unblocked for bona fide legitimate purposes.

Another useful complexity derives from the flexible relationship between public institutions, private corporations, government discounts, and noncommercial developers. Most public institutions purchase licenses for filtering systems built and maintained by external organizations. As discussed briefly in Strategy A, and covered more extensively by Zittrain and Palfrey's (2008) review of commercial filtering software, there are strong business incentives involved: The information security companies that provide filtering are routinely valued in the hundreds of millions of dollars, and business is booming in the current era of concern over hacking and malware. Of our respondents, five provided information about their contracts with filtering companies:

- Eve County Schools pays $6,160 annually for 1,100 Sophos licenses.
- Frank Public Library pays $655 annually for 50 iPrism (a product of EdgeWave) licenses.
- David City Schools pays $3,483 annually for Internet service, including filtering, provided at no discount by Alabama Supercomputer Authority.
- Grace County Public Library pays $828 annually for Internet service, including filtering, provided at a 77% discount by Alabama Supercomputer Authority.
- Heidi Public Library pays $870 annually for Internet service, including filtering, provided at an 80% discount by Alabama Supercomputer Authority.

Of these, Sophos is a publicly traded British company with annual revenues of ~$450 million in 2015, whereas EdgeWave is a privately held American company without public revenue numbers. By comparison, Alabama Supercomputer Authority (ASA) is a state-funded nonprofit corporation that offers telecommunications services to Alabaman schools and libraries. More than half of our respondents indicate they rely on ASA for their filtering services. However, this too is a regress: According to ASA, they subcontract their filtering to iBoss, a privately held cybersecurity company valued at ~$500 million in 2015 (Alabama Supercomputer Authority, n.d.) The nesting doll nature of filtering companies not only creates confusion among patrons and administrators as to which agency is responsible for any given filtering outcome but also operates in direct contradiction to professional norms forbidding librarians from outsourcing content selection to private entities (Batch, 2014).

Not all filtering providers are multinational information security corporations, however. Consider the case of DansGuardian, which is, as it turns out, a free and open-source content filtering system coded by a man named Dan. According to his "How I Did It" page, around the year 2000 Dan thought that other content filtering providers were "rubbish," so he learned C++ and built one himself. The product, Dan promises, "filters the actual content of pages . . . [not] on a banned list of sites like lesser totally commercial filters. DansGuardian is designed to be completely flexible and allows you to tailor the filtering to your exact needs" (DansGuardian, 2011, p. 2; see Figure 9). Although Dan is now CTO of a private filtering company and no longer maintains his eponymous project, the software remains freely available and actually implemented to achieve CIPA compliance by at least two Alabaman public libraries.

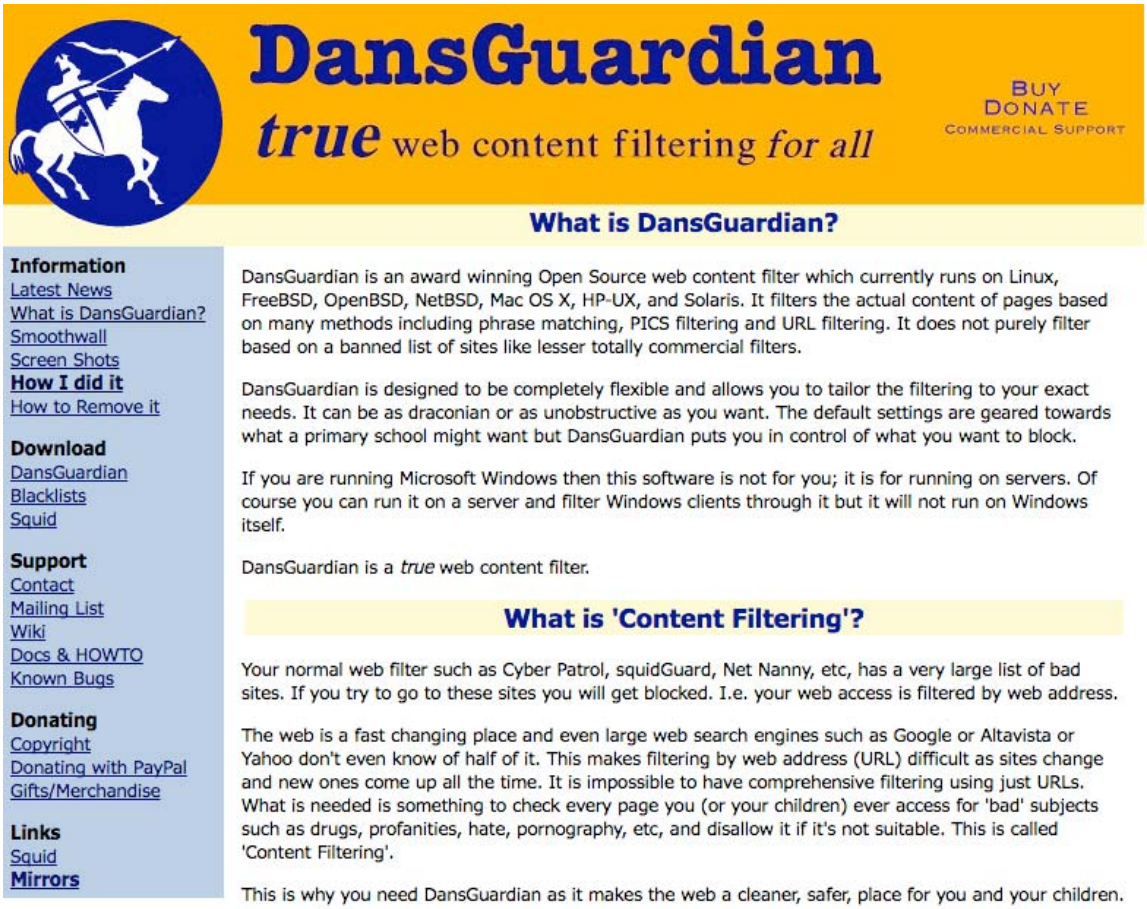


Figure 9. An explanation of DansGuardian, written by Dan.

While Dan locates filtering agency "in" his code, other providers distribute it across a network of actors. In a corporate blog post addressing CIPA compliance, a Barracuda employee assures administrators that its "preclassified" blacklist of URLs is "continuously updated by engineers at Barracuda Central and delivered hourly via the Energize Updates subscription service sold with the Barracuda Web Filter," which can then be manipulated further by local technicians (Barry, 2015, p. 5). Indeed, the marketing materials of filtering companies at once presume and reflect the complexity of filtering systems, prescribing local administrators toggling categories populated by algorithms, coded by engineers, to meet a market opportunity induced by federal legislation, impelled by moral panics, implemented by understaffed institutions, to serve fickle patrons.

When viewed from this perspective, it seems unsurprising (even inevitable) that this long chain of associations can produce inconsistent filtering results; indeed, their complexity makes it almost inevitable. As the anthropologist Nick Seaver (2013) observes:

> When we realize that we are not talking about algorithms in the technical sense, but rather algorithmic systems of which code *strictu sensu* is only a part, their defining features reverse: instead of formality, rigidity, and consistency, we find flux, revisability, and negotiation. . . . These algorithmic systems are not standalone little boxes, but massive, networked ones with hundreds of hands reaching into them, tweaking and tuning, swapping out parts and experimenting with new arrangements. (p. 10)

While Seaver was writing primarily on the topic of social media systems, the same dynamic obtains for the filtering systems implemented by public institutions.

Conclusion

In this article, we shared the results of a study of Internet filtering configurations in Alabama public schools and libraries. We compared configurations of the same TPMs across different institutions, as well as different TPMs across different institutions, to demonstrate significant inconsistencies in the kinds of content blocked or permitted by them. We demonstrated that these inconsistencies are produced by differentiations in the design and implementation of filtering systems across institutions that make strategic use of categories, lists, and complexity to perform the anticipation, articulation, and interpretive work required of institutions charged with making information (un)available.

Our findings are significant for two reasons. First, they contribute to the Internet filtering literature by showing how, and what kinds of, inconsistencies arise in the everyday work of Internet filtering. As we discussed in our literature review, prior studies have largely treated filters as stable, universal objects that are either adopted or not, or examined individual filters with global settings "built into" the software to assess "error rates." By comparing specific, local implementations of filtering systems, and illuminating the complex network of actors entangled within them, we have illustrated a more detailed picture of how filters, and those who configure them, work to simultaneously produce local order and global disorder. The inconsistencies that arise in Internet filtering are not merely the result of "errors" in their software but the product of different design choices in category schemas driven by market competition, as well as different configuration choices made by local administrators driven by institutional preferences.

As such, the effect of Internet filtering practiced by our respondents often reaches far beyond the narrow social function contemplated by Congress with CIPA or approved by the Supreme Court that upheld it, a finding consistent with recent ALA reports on overbroad filtering (Batch, 2014). This finding is troubling because it supports the conclusion that public subsidies both require and fund a broader form of arbitrary institutional control over information than was ever publicly legislated or litigated. As people who work as and with librarians, we understand, and are sympathetic to, the practical difficulties faced by administrators who must balance many competing (and sometimes contradictory) norms in the course of their jobs. However, with this article we hope to illuminate the gap between the text of the law and its implementation to help reinvigorate the legal and professional debates about how and why Internet filtering is and ought to be practiced by public institutions.

The second reason our finding is significant is that the inconsistent access to information mediated by the TPMs of public institutions resembles other inconsistencies in the information made (un)available through other contemporary intermediaries. As discussed in our introduction, there is a rapidly developing body of literature in communication and media studies investigating (a) how certain information is made more or less visible through social media, search engines, and other networked information intermediaries; (b) which agents determine this visibility/availability; and (c) the potential implications for democracy. These questions remain contested: One of the more comprehensive recent reviews was conducted by Flaxman, Goel, and Rao (2016), who "uncovered evidence for both sides of the debate" (p. 318) as to whether contemporary information access patterns encourage the integration or dissolution of what Benkler (2006) famously described as a networked public sphere.

It is outside the scope of this article to resolve this ongoing debate. We do, however, want to link the inconsistencies observed across both private and public intermediaries as parallel phenomena. Recent literature regarding the consequences of curation have taken Twitter (Himelboim, McCreery, & Smith, 2013), Facebook (Bakshy, Messing, & Adamic, 2015), and cable news channels (Arceneaux & Johnson, 2013) as their subject to study how inconsistencies across intermediaries may influence different understandings of the world. Because public schools and libraries continue to play a major role as Internet intermediaries to millions of Americans, it seems reasonable to ask whether and how the inconsistent filtering practiced by these institutions influences the worldviews of those who rely on them for access.

Consider, for example, the sites and services mentioned in our introductory story. One of our respondents, a public school district, used Lightspeed and blocked "Adult" while permitting "Society.Politics." Another school district uses Websense and blocks "Entertainment" while permitting "News and Media." Because of how these systems categorize websites, and the category selections made by school administrators, this means that staff and students at these two schools are likely prevented from reading *Jezebel* or *Buzzfeed* at school while allowed to freely browse *Breitbart* and *InfoWars* with their publicly subsidized Internet. While we do not propose a crudely deterministic relationship for this kind of information environment, it is difficult to imagine that it is entirely without consequence, both for the individuals involved and the society in which they participate.

In future work, we intend to extend this project in several respects. First, as mentioned above, we hope to expand our current approach to a stratified sample of institutions from more states to cover more literal and figurative ground for additional analysis. Second, we anticipate that deeper qualitative work, particularly ethnography and/or interviews with institutional administrators and users, would further illuminate the rich complexity of their lived experiences more than our documentary traces can do. To this end, we look forward to a new project, announced while this article was being revised, by Kozak and Zimmer to conduct unstructured interviews regarding filtering implementation with public librarians in Wisconsin (Zimmer, 2017), which we believe will complement our work. Third, we hope to partner with other scholars, professional organizations, and other interested parties to reconsider the cultural work of Internet filtering in public institutions, with renewed focus on the influential intermediary role they play when it comes to learning about, and participating in, the common world.

References

Alabama Open Meetings Act. (2005). Retrieved from https://www.openmeetings.alabama.gov/generalpublic/downloads/Act2005-40.pdf

Alabama Supercomputer Authority. (n.d.). Content filtering. Retrieved from https://www.asc.edu/network/mia-services/content-filtering

All about *MexConnect*. (n.d.). Retrieved from http://www.mexconnect.com/pages/about

Ananny, M., & Crawford, K. (2016). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*. Advance online publication. Retrieved from doi:10.1177/1461444816676645

Annear, S. (2017, May 17). MIT student sues CIA for information about its social media jokes, use of Twitter. *The Boston Globe.* Retrieved from https://www.bostonglobe.com/metro/2017/05/17/mit-student-sues-cia-for-information-about-its-social-media-jokes-use-twitter/lt1RK85nyIBrSQbgILVNAP/story.html

Arceneaux, K., & Johnson, M. (2013). *Changing minds or changing channels? Partisan news in an age of choice*. Chicago, IL: University of Chicago Press.

Bakshy, E., Messing, S., & Adamic, L. A. (2015). Political science: Exposure to ideologically diverse news and opinion on Facebook. *Science*, *348*(6239), 1130–1132.

Barry, C. (2015, March 16). CIPA compliance with the Barracuda Web filter [Web log post]. Retrieved from https://blog.barracuda.com/2015/03/16/cipa-compliance-with-the-barracuda-web-filter/

Batch, K. R. (2014, June). *Fencing out knowledge: Impacts of the Children's Internet Protection Act 10 years later* (ALA Policy Brief No. 5). Retrieved from http://connect.ala.org/files/cipa_report.pdf

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Bertot, J. C., Jaeger, P., Lee, J., Dubbels, K., McDermott, A., & Real, B. (2014). *2013 Digital Inclusion Survey: Survey findings and results*. College Park, MD: Information Policy and Access Center, University of Maryland. Retrieved from http://digitalinclusion.umd.edu/sites/default/files/uploads/2013DigitalInclusionNationalReport.pdf

Bertot, J. C., Real, B., & Jaeger, P. T. (2016). Public libraries building digital inclusive communities: Data and findings from the 2013 Digital Inclusion Survey. *The Library Quarterly*, *86*(3), 270–289.

Bertot, J. C., Real, B., Lee, J., McDermott, A. J., & Jaeger, P. T. (2015). *2014 Digital Inclusion Survey: Survey findings and results*. College Park, MD: Information Policy and Access Center, College of Information Studies, University of Maryland. Retrieved from http://digitalinclusion.umd.edu/sites/default/files/uploads/2014DigitalInclusionSurveyFinalRelease.pdf

Bogost, I. (2012). *Alien phenomenology, or what it's like to be a thing*. Minneapolis, MN: University of Minnesota Press.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Brunton, F. (2013). *Spam: A shadow history of the Internet*. Cambridge, MA: MIT Press.

Caldwell-Stone, D. (2013, April 2). Filtering and the First Amendment. *American Libraries Magazine*. Retrieved from https://americanlibrariesmagazine.org/2013/04/02/filtering-and-the-first-amendment/

Children's Internet Protection Act, 47 U.S.C. §54.520 (2000). Retrieved from https://www.law.cornell.edu/cfr/text/47/54.520.

Clarke, A. E. (2016). Anticipation work: Abduction, simplification, hope. In G. C. Bowker, S. Timmermans, A. E. Clarke, & E. Balka (Eds.), *Boundary objects and beyond: Working with Leigh Star*. Cambridge, MA: MIT Press.

Comer, A. D. (2006). Studying Indiana public libraries' usage of Internet filters. *Indiana Libraries*, *25*(1), 19–23.

DansGuardian. (2011). Web filtering for all. Retrieved from http://dansguardian.org/

Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly*, *80*(S1), 298–320.

Friedman, M (2017). Steven Morgan Friedman. Retrieved from https://westegg.com/morgan/cv/

Geiger, R. S. (2011). The lives of bots. In G. Lovink & N. Tkacz (Eds.), *Wikipedia: A critical point of view* (pp. 78–93). Amsterdam, Netherlands: Institute of Network Cultures.

Gerson, E. M., & Star, S. L. (1986). Analyzing due process in the workplace. *ACM Transactions on Information and System Security*, *4*(3), 257–270.

Haraway, D. (1992). The promises of monsters: A regenerative politics for inappropriate/d others. In L. Grossberg, C. Nelson, & P. A. Treichler (Eds.), *Cultural studies* (pp. 295–337). New York, NY: Routledge.

Himelboim, I., McCreery, S., & Smith, M. (2013). Birds of a feather tweet together: Integrating network and content analyses to examine cross-ideology exposure on Twitter. *Journal of Computer-Mediated Communication*, *18*(2), 40–60.

Jaeger, P. T., Bertot, J. C., McClure, C. R., & Langa, L. A. (2006). The policy implications of Internet connectivity in public libraries. *Government Information Quarterly*, *23*(1), 123–141.

Jaeger, P. T., & Yan, Z. (2009). One law with two outcomes: Comparing the implementation of CIPA in public libraries and schools. *Information Technology and Libraries*, *28*(1), 6–14.

Johnson, A. (2017). *Twitter and the body parodic: Global acts of re-creation and recreation.* (Unpublished doctoral dissertation). Massachusetts Institute of Technology, Cambridge, MA.

Johnson, J. (1988). Mixing humans and nonhumans together: The sociology of a door-closer. *Social Problems*, *35*(3), 298–310.

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Cambridge, MA: Harvard University Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network theory*. Oxford, UK: Oxford University Press.

Minow, M. (1997). Filters and the public library: A legal and policy analysis. *First Monday*, *2*(12). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/564/485

Minow, M. (2004). Lawfully surfing the Net: Disabling public library Internet filters to avoid more lawsuits in the United States. *First Monday*, *9*(4). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1132/1052

Mol, A. (2002). *The body multiple: Ontology in medical practice*. Durham, NC: Duke University Press.

O'Connor, A. (2012, August 29). Missourian publishes "unfit to read" banned book project [Web log post]. Retrieved from https://ncacblog.wordpress.com/2012/08/29/missourian-publishes-unfit-to-read-banned-book-project/

Oltmann, S. M., Knox, E. J. M., Peterson, C., & Musgrave, S. (2015). Using open records laws for research purposes. *Library & Information Science Research*, *37*(4), 323–328.

Oltmann, S.M., Peterson, C., & Knox, E. J. M. (2017). Analyzing challenges to library materials: An incomplete picture. *Public Library Quarterly.* Advance online publication. Retrieved from doi:10.1080/01616846.2017.1324233

Pariser, E (2011). *The filter bubble: How the new personalized Web is changing what we read and how we think*. New York, NY: Penguin Books.

Peterson, C. (2013, October 25). Mapping banned books in Massachusetts: We asked every public school and library in the state about banned books, and here's what they said [Web log post]. Retrieved from https://civic.mit.edu/blog/petey/mapping-banned-books-in-massachusetts-we-asked-every-public-school-and-library-in-the

Resnick, P. J., Hansen, D. L., & Richardson, C. R. (2004). Calculating error rates for filtering software. *Communications of the ACM*, *47*(9), 67–71.

Schneier, B. (1996). Applied cryptography: Protocols. *Algorithms, and Source Code in C*, *2*, 216–222.

Seaver, N. (2013). Knowing algorithms. *Media in Transition 8*, 1–12.

Star, S. L. (1999). The ethnography of infrastructure. *The American Behavioral Scientist*, *43*(3), 377–391.

Sunstein, C. R. (2009). *Republic.com 2.0*. Princeton, NJ: Princeton University Press.

Trustwave. (2014, August 17). Trustwave Web filtering content categories. Retrieved from https://www.trustwave.com/Resources/Library/Documents/Trustwave-Web-Filtering-Content-Categories/

United States v. American Library Assn., Inc., 539 U.S. 194 (2003).

Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the Children's Internet Protection Act? *Journal of Applied Developmental Psychology*, *30*(3), 209–217.

Zimmer, M. (2017, April 3). New project: Assessing the implementation of CIPA-mandated Internet filtering in U.S. public libraries. *MichaelZimmer.org*. Retrieved from http://www.michaelzimmer.org/2017/04/03/assessing-the-implementation-of-cipa-mandated-internet-filtering-in-public-libraries/

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, & J. G. Stein (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 29–56). Cambridge, MA: MIT Press.