

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

SARAH BRADBURN, PEARL
CHERRINGTON, CHARLES HEINLEN,
and the SECOND AMENDMENT
FOUNDATION,

Plaintiffs,

v.

NORTH CENTRAL REGIONAL LIBRARY
DISTRICT,

Defendant.

No. CV-06-327-EFS

**PLAINTIFFS’ COUNTERSTATEMENT
OF FACTS IN OPPOSITION TO
DEFENDANT’S MOTION FOR
SUMMARY JUDGMENT**

Plaintiffs Sarah Bradburn, Pearl Cherrington, Charles Heinlen and the Second Amendment Foundation submit the following Counterstatement of Facts in Opposition to Defendant’s Motion for Summary Judgment.

1. To clarify Defendant’s Fact #7: NCRL’s Board of Directors has delegated certain tasks to Dean Marney, Director of the North Central Regional Library District (“NCRL”) – including determining what categories and classifications of Web sites should be blocked by NCRL’s FortiGuard filter. See Howard Dep. at 44:4-7, 50:9-17 (Ct. Rec. 41 at 220, 221); Walters Dep. at 18:20-22, 52:23-53:24 (Ct. Rec. 41 at 292, 297-98).

1 2. Plaintiffs object to NCRL’s assertion in its Fact #15 that it is “responsible” for
2 “working cooperatively with public schools in its territory.” NCRL cites no authority – legal
3 or otherwise – to support the assertion.

4 3. With regard to Defendant’s Fact #21: Plaintiffs object that the Children’s
5 Internet Protection Act (“CIPA”) speaks for itself. Moreover, the definition of “technology
6 protection measure” in CIPA is narrower than NCRL suggests. CIPA § 1703(b)(1) states in
7 pertinent part: “The term ‘technology protection measure’ means a specific technology that
8 blocks or filters Internet access to visual depictions that are: (A) obscene, as that term is
9 defined in section 1460 of title 18, United States Code; (B) child pornography, as that term is
10 defined in section 2256 of title 18, United States Code; or (C) harmful to minors.” CIPA §
11 1703(b)(2) in turn defines “harmful to minors” to mean “any picture, image, graphic image
12 file, or other visual depiction that – (A) taken as a whole and with respect to minors, appeals
13 to a prurient interest in nudity, sex, or excretion; (B) depicts, describes, or represents, in a
14 patently offensive way with respect to what is suitable for minors, an actual or simulated
15 sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd
16 exhibition of the genitals; and (C) taken as a whole, lacks serious literary, artistic, political, or
17 scientific value as to minors.” In sum, CIPA defines “technology protection measure” as a
18 technology that blocks or filters Internet access to “visual depictions” that are obscenity, child
19 pornography or harmful to minors.

20 4. With regard to Defendant’s Fact #22: Plaintiffs object that CIPA speaks for
21 itself. Two similar statutory provisions are at issue. 20 U.S.C. § 9134(b)(3) provides: “An
22 administrator, supervisor, or other authority may disable a technology protection measure
23 under paragraph (1) to enable access for bona fide research or other lawful purposes.” 47
24 U.S.C. §254(h)(6)(D) reads: “An administrator, supervisor, or other person authorized by the
25 certifying authority under subparagraph (A)(i) may disable the technology protection measure
26 concerned, during use by an adult, to enable access for bona fide research or other lawful

1 purpose.” The circumstances in which CIPA allows for disabling of a library Internet filter
2 are thus quite broad: under CIPA, the filter may be disabled at the request of a library patron
3 who wishes to use the Internet for any lawful purpose. Finally, although CIPA may not, on its
4 face, require that library Internet filters be disabled at the request of adults, the First
5 Amendment of the United States Constitution and Art. I, § 5 of the Washington State
6 Constitution require such disabling.

7 5. Plaintiffs object to Defendant’s Fact #23 – particularly the paragraph’s
8 preamble – as argumentative and unsupported by authority. In particular, NCRL cites no
9 authority for its suggestion that it possesses “broad discretion to decide what material to
10 provide to its patrons in fulfillment of its mission.” Plaintiffs deny that NCRL possesses such
11 “broad discretion” in the context of Internet filtering – and particularly with regard to whether
12 NCRL’s Internet filter must be disabled at the request of adults. Nor does NCRL cite any
13 authority for its suggestion that full-time Internet filtering is necessary to “create a safe
14 environment for its patrons and employees,” or for its suggestion that its policy of never
15 disabling its Internet filter at the request of adult patrons is consistent with its obligations
16 under CIPA. Contrary to the implication in Defendant’s Fact #23, CIPA does not require or
17 permit NCRL to configure its Internet filter to block an enormous quantity of constitutionally-
18 protected speech, and does not require or permit NCRL to deny requests by adults to have the
19 filter disabled.

20 6. Contrary to Defendant’s Fact #27:

21 NCRL’s Director, Dean Marney, testified at deposition that NCRL first made the
22 Internet available to its patrons in the late 1990s. See Marney Dep. at 39:11-15 (Ct. Rec. 41 at
23 237). Mr. Marney’s deposition testimony was consistent with documents produced by NCRL
24 in discovery showing that NCRL’s Omak branch went online in November 1999, see Minutes
25 of November 17, 1999 meeting of NCRL’s Board of Directors, at NCRL 00296 (Ex. XX); and
26 that NCRL’s largest branch (in Wenatchee) went online in January 2000, see January 13,

1 2000 Director's Report, at NCRL 00301 (Ex. YY). Mr. Marney's testimony was also
2 consistent with a series of letters that he sent to Nancy Talner of the American Civil Liberties
3 Union of Washington in 2000. See Correspondence from Mr. Marney to Ms. Talner (Ex.
4 CCC).

5 Mr. Marney also testified at deposition that public Internet access on NCRL's
6 computers has been continuously filtered since NCRL first made the Internet available to its
7 patrons in the late 1990s

8 Q. I see. Do you recall when the NCRL first put it's Internet filter in place?

9 A. We've never had unfiltered access so –

10 Q. From –

11 A. – from the inception.

12 Q. Okay. So the first day you went – went online –

13 A. Went online.

14 Q. – it was filtered?

15 A. That's my recollection.

16 Marney Dep. at 109:24-110:7 (Ex. RR); see also id. at 81:14-17, 82:23-25, 84:3-16 (Ct. Rec.
17 41 at 248); Dep. Ex. 3 (Ct. Rec. 41 at 302); Defendant's Discovery Responses, answer to
18 Interrogatory No. 4 (Ct. Rec. 41 at 104-06). Documents produced by NCRL in discovery
19 corroborate this testimony. Those documents show that on June 10, 1999 NCRL's Board of
20 Directors approved an Internet Public Use Policy that provided for Internet filtering, and
21 specifically instructed Mr. Marney to install a filtering system on all of NCRL's public access
22 computers. See Minutes of June 10, 1999 meeting of NCRL's Board of Directors, at NCRL
23 00277 (Ex. VV). The documents further show that filtering software had been ordered and
24 received by August 12, 1999. See Minutes of August 12, 1999 meeting of NCRL's Board of
25 Directors, at NCRL 00281 (Ex. WW). The letters that Mr. Marney sent to Ms. Talner in 2000
26

1 further confirm that Internet access on NCRL's computers was filtered well before December
2 2000. See Ex. CCC.

3 7. Contrary to Defendant's Fact #28: Documents produced by NCRL in
4 discovery indicate that the first filtering product that NCRL purchased was SurfWatch, not
5 N2H2's SmartFilter, Bess Edition. See Minutes of May 11, 2000 meeting of NCRL's Board
6 of Directors, at NCRL 00313 (Ex. ZZ). Mr. Marney's letters to Ms. Talner in 2000 confirm
7 that NCRL's first filtering product was SurfWatch. See Ex. CCC. NCRL was using the
8 N2H2 filtering product by January 11, 2001. See January 11, 2001 Director's Report, at
9 NCRL 00334 (Exhibit AAA); Minutes of January 11, 2001 meeting of NCRL's Board of
10 Directors, at NCRL 00332 (Exhibit BBB); Defendant's Discovery Responses, answer to
11 Interrogatory No. 1 (Ct. Rec. 41 at 100-02); February 6, 2001 letter from Mr. Marney to Ms.
12 Talner (Exhibit CCC).

13 8. Plaintiffs object to Defendant's Fact #29 on grounds of hearsay and lack of
14 personal knowledge.

15 9. Contrary to Defendant's Fact #30: Although many of the specific incidents
16 giving rise to the current litigation occurred while the Bess filter was in place, NCRL
17 continued to block a substantial number of Web sites after implementing its current
18 FortiGuard filter – including sites that Plaintiffs wished to access. See Cherrington Dep. at
19 33:16-34:8 (Ct. Rec. 41 at 182); Cherrington's Discovery Responses, answers to Interrogatory
20 Nos. 5, 8, 9, 11, 12 (Ct. Rec. 41 at 60-63) (FortiGuard denied Plaintiff Pearl Cherrington
21 access to YouTube); Heinlen Dep. at 22:25-24:10, 29:7-12, 31:7-14, 63:13-73:21 (Ct. Rec. 41
22 at 200, 202, 206-09); Heinlen's Discovery Responses, answers to Interrogatory Nos. 5, 11, 12
23 (Ct. Rec. 41 at 72-76, 79) (FortiGuard denied Plaintiff Charles Heinlen access to MySpace,
24 various dating sites, images embedded in emails, and many other miscellaneous Web sites).
25 NCRL has submitted no evidence showing that the majority of Web sites to which Mr.
26 Heinlen was previously denied access have been unblocked.

1 10. Plaintiffs object to Defendant's Fact #39 on the grounds that it constitutes
2 hearsay, is so vague as to be meaningless, and improperly purports to state a legal conclusion.
3 Additionally, no Exhibit F was attached to Dr. Resnick's declaration (nor, for that matter, was
4 any Exhibit E attached to his declaration). And finally, the Fortinet witness whom NCRL's
5 counsel deposed on January 17, 2008 testified that to the best of his knowledge, "there is no
6 certification process for actual products with regards to CIPA." Deposition of Liam Chasteen
7 ("Chasteen Dep.") at 37:3-5 (Ex. NN); see also id. at 35:25-37:16.

8 11. To clarify Defendant's Fact #54: On February 23, 2008 Plaintiff Charles
9 Heinlen visited NCRL's Omak branch to determine whether certain Web sites were blocked
10 by NCRL's Internet filter. See Declaration of Charles Heinlen in Opposition to Defendant's
11 Motion for Summary Judgment ("Heinlen Decl. in Opp.") at ¶ 3. He attempted to access the
12 following Web sites, and confirmed that the FortiGuard filter currently blocks all of them
13 under the category Nudity and Risque, except www.courting-disaster.com which is blocked
14 under the category Adult Materials:

15 www.netnude.com
16 aanr.com
17 www.artenuda.com/paintings2.asp
18 gregfriedler.com
19 billbrandt.com
20 www.ryoung-art.com
21 www.courting-disaster.com
22 www.mapplethorpe.org/index.html
23 fineartnude.com/webring

24 Id. Copies of screen shots of the splash pages of the above-listed Web sites are attached
25 hereto as Exhibit DDD. Mr. Heinlen also attempted to access the personals section of the
26 Craigslist Web site, but NCRL's filter denied him access to that site as well. See Heinlen
Decl. in Opp. at ¶ 3. Mr. Heinlen wishes to access that section of the Craigslist site in the
future. Id.

1 12. With regard to Defendant's Fact #55, the definitions listed in that paragraph
2 contain several non-substantive typographical errors, and do not precisely match the
3 definitions provided by Fortinet on its Web site and listed in the document attached as Exhibit
4 C to Barbara Walters' declaration.

5 13. Plaintiffs object to Defendant's Fact #59 because it is based on the declaration
6 of Dean Marney, who has no personal knowledge of when Dan Howard (who responded to all
7 the unblocking requests that NCRL received after October 1, 2007) actually answered the
8 requests. Moreover, contrary to, and by way of clarification of Defendant's Fact #59:

9 A review of documents recently produced by NCRL indicates that NCRL received 92
10 unblocking requests (including 90 automated requests) between October 1, 2007 and February
11 20, 2008. (NCRL received 83 automated requests before it filed its Motion for Summary
12 Judgment on February 4, 2008.) Copies of those documents are attached hereto as Exhibit
13 EEE. The various requests and NCRL's responses to them are summarized in the spreadsheet
14 that is attached hereto as Exhibit FFF. Based on the documents in Exhibit EEE (and as
15 summarized in Exhibit F):

- 16 • Of the 90 automated unblocking requests that NCRL received between
17 October 1, 2007 and February 20, 2008, NCRL responded to 25 requests
18 more than 24 hours after they were received (in some cases the delay
19 stretched to more than three days).
- 20 • Of the remaining 65 requests, NCRL responded to 29 requests the next day.
- 21 • Of the remaining 36 requests, NCRL responded to 27 requests on the same
22 day they were received (with two responses going out by mail), but in only
23 eight instances did NCRL respond in less than an hour.
- 24 • It cannot be determined whether NCRL responded to the remaining 11
25 requests.
- 26 • NCRL has granted a patron's request to unblock a Web site on only 12
 occasions since October 1, 2007.
- Web sites that have been blocked in error and about which NCRL patrons
 have specifically complained since October 1, 2007 include
 www.keyartpromotions.com, artbyjohndan.com (described by the requestor
 as "non-offensive, mostly abstract art"), www.pcthandbook.com
 (erroneously blocked as "Pornography"), www.firstthings1st.com

1 (described by the requestor as a nonprofit ministry but erroneously blocked
2 as “Gambling”), and www.ourfamily-web.com (erroneously blocked as
3 Malware).

- 4 • NCRL has refused to unblock numerous image search sites despite having
5 received requests by library patrons to be allowed to view images:
 - 6 - for scrapbooking,
 - 7 - of Disney characters,
 - 8 - needed to study for anatomy and physiology,
 - 9 - to help in quilting,
 - 10 - needed to do homework for college,
 - 11 - relating to law enforcement,
 - 12 - of the Normandy beaches at the time of D-Day,
 - 13 - of singer Gerard Way, and
 - 14 - of Michael Jordan.

- 15 • NCRL has also refused requests by its patrons to unblock:
 - 16 - Chat sites (including sites like www.meebo.com that do not require
17 users to download software);
 - 18 - www.animeinsider.com, not because the site had pornographic
19 material on it, but merely because it had links to other sites that Dan
20 Howard considered pornographic; and
 - 21 - www.happyhacker.org, because it included sections that appeared
22 to give hacking tips. This despite the fact that the site bills itself as
23 “The website computer criminals don’t want you to read” and is
24 focused primarily on techniques for defending computers against
25 hackers. See Ex. DDD.

15 14. Contrary to Defendant’s Fact #60, NCRL’s policy of refusing to disable its
16 Internet filter at the request of adults is not consistent with its mission to promote reading and
17 lifelong learning. NCRL’s policy is guaranteed to prevent adults from reading and learning
18 about topics that NCRL has placed off limits from all its patrons. Plaintiffs also deny that
19 there is any connection between “NCRL’s current filtering profile” and the safety of NCRL’s
20 library branches. NCRL has adduced no evidence of any such connection.

21 15. Contrary to Defendant’s Fact #61, NCRL’s policy does not comply with CIPA.
22 As Plaintiffs explained in footnote 1 to their Memorandum of Law in Support of Their Motion
23 for Summary Judgment, NCRL’s filtering policy conflicts with CIPA in numerous respects.

24 16. Plaintiffs object to Defendant’s Fact #62 on the grounds that CIPA speaks for
25 itself, and that in testifying about what CIPA requires Mr. Marney (on whose testimony this
26 paragraph is based) is impermissibly purporting to state a legal conclusion.

1 17. Plaintiffs object to Defendant’s Fact #63 on the ground that CIPA speaks for
2 itself, and that in testifying about what CIPA requires Mr. Marney (on whose testimony this
3 paragraph is based) is impermissibly purporting to state a legal conclusion. Plaintiffs further
4 object that this paragraph does not accurately summarize the relevant portions of CIPA.

5 18. Plaintiffs object to Defendant’s Fact #64 on the ground that CIPA speaks for
6 itself, and that in testifying about what CIPA requires Mr. Marney (on whose testimony this
7 paragraph is based) is impermissibly purporting to state a legal conclusion. Plaintiffs further
8 object that this paragraph does not accurately summarize the relevant portions of CIPA.

9 19. Plaintiffs object to Defendant’s Fact #65 on the ground that CIPA speaks for
10 itself.

11 20. Plaintiffs object to Defendant’s Fact #66 as vague, conclusory and lacking
12 foundation. The paragraph is predicated solely on the declaration of Dean Marney, who
13 testified at deposition that technical questions relating to NCRL’s FortiGuard filter would be
14 better addressed to the library’s Information Technology Manager, Barbara Walters, see
15 Marney Dep. at 121:16-20 (Ct. Rec. 41 at 255); and that he did not know what the procedure
16 would be for disabling the filter on one of NCRL’s public use computer terminals, id. at
17 109:406 (Ex. RR).

18 Moreover, contrary to Defendant’s Fact #66, disabling the FortiGuard filter at the
19 request of adults would be consistent with NCRL’s mission. NCRL’s assertion that disabling
20 the filter at the request of adults would present “other problems” is so vague and conclusory
21 as to be entirely meaningless.

22 As for NCRL’s contention that disabling the FortiGuard filter would present
23 unspecified “technological challenges,” that contention is inconsistent with the facts that have
24 been developed through discovery. Fortinet representative Liam Chasteen testified as follows
25 at deposition:

26 Q. Can a librarian at a particular library branch that is using the FortiGuard
filter disable the filter on a particular computer terminal?

1 A. Yes.

2 Q. How would a librarian go about doing that?

3 A. Depending on how the FortiGate was configured, it could be as simple as
4 merely logging in and checking a check box.

5 Q. That would allow a library patron to have unfiltered Internet access at that
6 terminal; correct?

7 A. If properly configured; correct.

8 Chasteen Dep. at 57:5-15 (Ex. NN); see id. at 61:8-11.

9 It also bears noting that, as Mr. Marney testified at deposition, although Internet access
10 at all of NCRL's staff computers is filtered, NCRL is able to disable the filter on at least some
11 of its computers to allow staff members to view Web sites to which NCRL's patrons have
12 requested access:

13 Q. What's the NCRL's filtering policy with regard to staff terminals?

14 A. They're all filtered. CIPA requires that. Obviously, we have computers
15 here that the filter gets turned off so we can view those sites that are
16 blocked.

17 Q. Are the filters on the staff terminals ever turned off at any other time?

18 A. I don't know.

19 Q. What would be the procedure for disabling a filter on a staff terminal?

20 A. The – I don't know.

21 Q. Is there –

22 A. I'd ask Barbara.

23 Q. Okay. Do you know what the procedure would be for disabling the filter
24 on a public use terminal?

25 A. I do not know.

26 See Marney Dep. at 108:16-109:6 (Ex. RR). If NCRL can disable the FortiGuard filter on a
staff terminal, it should certainly be able to disable the filter on a public use terminal –
particularly where Fortinet's representative Mr. Chasteen testified that such disabling would
be a simple matter.

1 21. Plaintiffs object to Defendant’s Fact #67 based on lack of foundation (see
2 discussion of Defendant’s Fact #66 above) and because the paragraph is impermissibly vague
3 and conclusory. Moreover, it bears noting that NCRL does not dispute that it could acquire
4 the capacity to disable its FortiGuard filter at the request of adults by purchasing of additional
5 unspecified authentication software or hardware.

6 22. Plaintiffs object to NCRL’s reference in its Fact #69 to unidentified
7 “technological challenges” and the possibility of NCRL’s computer network being
8 “dismantled” for the reasons stated in their discussion of Defendant’s Fact #66 above.
9 Moreover, although, as Plaintiffs noted in their Motion for Summary Judgment at 3 n.2, they
10 do not dispute that NCRL may take appropriate steps to safeguard its computer network,
11 contrary to Defendant’s Fact #69 disabling the FortiGuard filter at the request of adult library
12 patrons would not pose any security threat to the network. See Declaration of Bennett
13 Haselton In Opposition to Defendant’s Motion for Summary Judgment.

14 23. Contrary to Defendant’s Fact #71, allowing unfiltered Internet access at the
15 request of adults would not create any unacceptable risks for NCRL’s patrons or staff, or
16 create a hostile atmosphere for families, children or staff. NCRL has adduced no evidence
17 that allowing unfiltered Internet access at the request of adults would create any such
18 unacceptable risks or hostile atmosphere.

19 24. Contrary to Defendant’s Fact #74, allowing unfiltered Internet access at the
20 request of adults would put not NCRL staff in the position of “being unwelcomingly exposed
21 to, and put in the position of, having to confront patrons.”

22 25. To clarify Defendant’s Fact #77, Dan Howard’s experience with privacy
23 screens is limited to a period when he worked for the Sno-Isle Regional Library between 1996
24 and 2001. See Howard Dep. at 27:2-8 (Ct. Rec. 41 at 215). He was not employed by NCRL
25 when NCRL briefly experimented with privacy screens at its Wenatchee branch in early 2000.
26 See Marney Dep. at 46:22-47:13 (Ct. Rec. 41 at 239); January 13, 2000 Director’s Report, at

1 NCRL 00301 (Ex. YY); Howard Dep. at 26:23-27:1 (Ct. Rec. 41 at 215). He has had no
2 experience with privacy screens since 2001, see Howard Dep. at 29:15-17 (Ct. Rec. 41 at
3 216); and has not research privacy screens since then, id. at 32:11-13 (Ct. Rec. 41 at 216).

4 26. To clarify Defendant's Fact #82, Mr. Howard's experience using recessed
5 desks is limited to the period between 1996 and 2001 when he worked for the Sno-Isle
6 Regional Library. See Howard Dep. at 35:5-19 (Ct. Rec. 41 at 217). He does not know if
7 recessed-desk technology has changed since 2001. Id. at 36:6-9 (Ct. Rec. 41 at 217).

8 27. Plaintiffs object to Defendant's Fact #84 because it is based on the hearsay
9 testimony of Dan Howard, who "looked up the price" of recessed desks on October 17, 2007
10 and testified at deposition (and reiterated in paragraph 23 of his declaration submitted in
11 support of NCRL's Motion for Summary Judgment) that with regard to a particular brand of
12 recessed desk called the Nova desk, "they start for very small ones at about a thousand dollars
13 apiece." Howard Dep. at 35:12-13 (Ct. Rec. 41 at 217). Should the Court decide to consider
14 Mr. Howard's hearsay testimony regarding the price of recessed desks, Plaintiffs ask that the
15 Court also consider the documents attached hereto as Exhibit GGG. These documents were
16 printed off the World Wide Web on February 23, 2008. See Declaration of Duncan Manville
17 in Opposition to Defendant's Motion for Summary Judgment ("Manville Decl. in Opp.") at ¶
18 23. They show that contrary to Mr. Howard's testimony, Nova recessed desks can be
19 purchased for as little as \$645 – not including discounts that might be available for bulk
20 purchases. The documents attached hereto as Exhibit GGG also show that other brands of
21 recessed desks are available for as little as \$539.99, and that side-by-side Nova recessed desks
22 (which NCRL could use at library branches with multiple public use terminals) are available
23 for as little as \$1,130, or \$565 per computer. Finally, another option that NCRL could
24 potentially avail itself of is retrofitting existing computer tables with hardware that would
25 allow NCRL to recess computer monitors in the existing tables. The documents attached
26 hereto as Exhibit GGG show that Nova retrofit kits are available for as little as \$392.

1 28. Plaintiffs object to Defendant’s Fact #89 as vague and conclusory. NCRL has
2 presented no evidence regarding how much more prevalent the incidents referenced in its Fact
3 #89 allegedly were before NCRL decided to configure its FortiGuard filter to block the Image
4 Search classification. In fact, contrary to Defendant’s Fact #89, during the course of this
5 litigation NCRL has identified by approximate date (that is, by month and year) only three
6 instances in which allegedly pornographic images were accessed online in an NCRL library
7 branch, and all three incidents took place after NCRL began blocking the Image Search
8 classification in January 2007 (see Defendant’s Fact #92 and Fact #96, referencing incidents
9 in March and December 2007 in which patrons were allegedly able to access pornography
10 online at NCRL’s Okanogan and Bridgeport branches; Howard Dep. at 39:13-41:1 (Ct. Rec.
11 41 at 218-19), referencing an incident in the Wenatchee branch that allegedly occurred within
12 the month prior to Mr. Howard’s October 17, 2007 deposition).

13 29. Plaintiffs object to Defendant’s Fact #90 through Fact #98 because they are
14 predicated solely on declaration testimony by Mr. Howard that is hearsay and is not based on
15 personal knowledge. In fact, these paragraphs, and the declaration testimony on which they
16 are predicated, are in many instances double hearsay, since Mr. Howard’s testimony appears
17 to be based in part on information that was allegedly communicated by unidentified staff
18 members to Sharron Reddick and several other named individuals who subsequently spoke
19 with Mr. Howard about what they had heard.

20 30. Plaintiffs also object to Defendant’s Fact #90 through Fact #98 and Mr.
21 Howard’s corresponding declaration testimony as vague and conclusory. For example, with
22 regard to Fact #91, NCRL and Mr. Howard do not say how many alleged “specific incidents”
23 occurred in which allegedly pornographic images were viewed online, or when the alleged
24 incidents occurred. NCRL and Mr. Howard do not describe the particulars of the alleged
25 incidents, or describe the allegedly “explicit, pornographic images” referenced in this
26 paragraph. The alleged images could have been anything from obscenity to harmless artistic

1 nudes. And finally, NCRL and Mr. Howard do not describe any of the “confrontations” that
2 allegedly took place, or provide any basis for concluding that the alleged “confrontations”
3 were of a nature that would have been stressful or upsetting to a librarian of ordinary and
4 reasonable sensibilities. For all that can be gleaned from Mr. Howard’s declaration, the
5 “confrontations” could very well have consisted of nothing more than polite dialogue.

6 Similarly, NCRL and Mr. Howard do not describe the particulars of the “inappropriate
7 pornographic materials” that were allegedly seen on the computers and printers at NCRL’s
8 Okanogan branch (Defendant’s Fact #93), do not describe the circumstances in which the
9 images were found (in fact, paragraph 93 does not even state that the images were
10 downloaded from the Internet, as opposed to having been uploaded from a disk or CD-ROM
11 for the purpose of printing hard copies), and do not state how many times the referenced
12 materials were allegedly found or when they were found.

13 NCRL and Mr. Howard do not describe the particulars of the alleged pornography that
14 was purportedly accessed by a single patron at NCRL’s Republic branch (Defendant’s Fact
15 #94), do not describe the circumstances in which the patron allegedly accessed the
16 pornography, do not state when or how many times the patron allegedly accessed the
17 referenced materials, and provide no specifics concerning the reference to unidentified patrons
18 allegedly “manag[ing] to access an inappropriate site.”

19 With regard to Defendant’s Fact #95, NCRL and Mr. Howard do not say when the
20 alleged incident referenced in the paragraph occurred (other than that it occurred sometime
21 before fall 2006), and provide no particulars concerning the alleged pornography at issue (in
22 fact, paragraph 95 again does not even state that the images in question were downloaded
23 from a Web site). Similarly, NCRL and Mr. Howard provide no specifics regarding the
24 allegedly pornographic images referenced in Defendant’s Fact #96 and the corresponding
25 paragraph 14 in Mr. Howard’s declaration, other than the subjective and conclusory assertion
26 that “the pictures were sexual and extremely graphic.” Defendant’s Fact #97 does not say

1 what Carla Loreto searched for or explain how a presumably innocuous search yielded the
2 result complained of.

3 Finally, Defendant's Fact #98 and the corresponding paragraph 16 of Mr. Howard's
4 declaration do not say how frequently Katy Sessions saw pornography on the public Internet
5 computers at NCRL's Wenatchee branch, either before or after NCRL implemented its
6 FortiGuard filter. Based on this paragraph there could have been two instances before fall
7 2006 and one after. Moreover, Fact #98 and Mr. Howard's corresponding declaration
8 testimony are demonstrably inaccurate, since (as explained above in Plaintiffs' discussion of
9 Defendant's Fact #27) NCRL's Wenatchee branch did not go online until January 2000. Ms.
10 Sessions could not possibly have seen Internet pornography on the Wenatchee computers in
11 1998 or 1999, as Fact #98 suggests, nor could she have been taking unspecified "anti-anxiety
12 medication" to cope with "uncomfortable confrontations with patrons regarding the Internet"
13 during that period. And finally, once again Fact #98 and Mr. Howard's corresponding
14 declaration testimony contain no specifics concerning any of the "uncomfortable
15 confrontations" that allegedly occurred between patrons and Wenatchee staff regarding the
16 Internet. Again, based on NCRL's conclusory Fact #98 these "confrontations" could have
17 amounted to nothing more than polite dialogue.

18 31. Plaintiffs also object to Defendant's Fact #90 through Fact #98 and to the
19 corresponding paragraphs in Mr. Howard's declaration on the grounds that none of the
20 librarians named in those paragraphs (Sharron Reddick, Jennifer Thompson, Lucile Ames,
21 Gailene Hooper, Claire Kirkpatrick, Michelle Orosco, Carla Loreto and Katy Sessions) were
22 disclosed by NCRL pursuant to Rules 26(a)(1)(A) or 26(e) as "individual[s] likely to have
23 discoverable information that the disclosing party may use to support its claims or defenses."
24 See Manville Decl. in Opp. at ¶ 27. Moreover, Mr. Howard was explicitly asked during his
25 October 17, 2007 deposition whether he was aware of any instances in which patrons of
26 NCRL had viewed pornographic images online and been requested to stop by NCRL staff.

1 See Howard Dep. at 39:13-42:11 (Ct. Rec. 41 at 218-19). Mr. Howard testified that he was
2 only aware of two such specific instances – one at NCRL’s Wenatchee branch and one at the
3 Omak branch. Id. He did not identify by name any of the persons allegedly involved. Id. He
4 stated that he was not aware of any instance in which a library patron had refused a request to
5 stop viewing inappropriate materials, and that he had no knowledge of there ever having been
6 any physical altercation or verbal dispute between library staff and a patron regarding the
7 viewing of inappropriate materials online. Id. To the extent Mr. Howard may have gathered
8 additional information (including the names of possible witnesses) since his October 17, 2007
9 deposition, that information was not disclosed to Plaintiffs until NCRL filed its Motion for
10 Summary Judgment on February 4, 2008. See Manville Decl. in Opp. at ¶ 27.

11 32. Finally, to clarify Defendant’s Fact #90 through Fact #98, it bears noting that
12 although NCRL first made the Internet available to its patrons at its Omak Branch over eight
13 years ago in December 1999 and at its Wenatchee branch in January 2000 (see above
14 discussion of Defendant’s Fact #27) and has had public Internet access in all of its library
15 branches since 2002 (see Defendant’s Discovery Responses, answer to Interrogatory No. 1
16 (Ct. Rec. 41 at 101)), NCRL has identified only two instances – referenced in its Fact #95 and
17 Fact #97 – in which a minor saw allegedly pornographic images on an NCRL public use
18 computer terminal. And in one of these instances the image was purportedly retrieved and
19 inadvertently shown to the minor by an NCRL staff member.

20 33. Contrary to Defendant’s Fact #99, under applicable law and on the facts
21 presented NCRL could not be held liable for facilitating a hostile work environment.

22 34. To clarify Defendant’s Fact #105, at deposition Dr. Resnick acknowledged that
23 the results of his study may have been skewed by the fact that the sample of URLs that he
24 used to generate his data was taken while the FortiGuard filter was in place:

25 Q. And why did you think it was appropriate to take a sample reflecting
26 patrons’ access patterns when the filters were installed?

1 A. Well, it depends what you are trying to test. So if you are trying to test in a
2 situation how many of the things that people try to access are done in error,
then it's good to take a list of what they actually access.

3 What you miss when you do that, and the reason I was bringing this up,
4 is that there may be things that people would have tried to access that they
5 don't try to access because they've had experience that they are blocked.
6 And if the filters had been around for a while, maybe the patrons have
adjusted their behavior. And I wouldn't be able to tell that from my study.
So any self-censorship that users are doing, I wouldn't be able to detect
with my study.

7 Deposition of Paul Resnick ("Resnick Dep.") at 92:12-93:2 (Ex. UU); see also id. at 93:3-
8 96:4.

9 35. To clarify Defendant's Fact #110:

10 As NCRL observes in its paragraph 106, in any given week there are approximately
11 2,180 instances in which an NCRL patron attempts to access a URL – either a complete Web
12 page or part of a Web page – and NCRL's FortiGuard filter denies the patron access to the
13 requested URL. It follows that NCRL patrons are denied access to Web pages and other
14 URLs 311 times every day, and 113,360 times every year.

15 A primary purpose of Dr. Resnick's study was to determine how many of the 2,180
16 URLs that the FortiGuard filter blocked during the week of August 23-29, 2007 were blocked
17 in error – that is, how many of those URLs should not have been blocked based on NCRL's
18 configuration of its filter and the categories and classifications that it had selected to block.
19 See Resnick report at 14 (Ct. Rec. 32 at 54).

20 To assess the FortiGuard filter's overblocking rate, Dr. Resnick and his colleagues
21 first had to classify the 2,180 URLs comprising the test set, and determine whether it would
22 be "possible to evaluate whether the URL should have been blocked." See Resnick report at
23 17-19 (Ct. Rec. 32 at 57-59). Dr. Resnick and his colleagues ultimately determined that of the
24 original test set of 2,180 URLs, only 2,070 were "ratable" – meaning that he and his
25 colleagues could determine whether they had been correctly blocked. See Resnick report at
26 19-20 (Ct. Rec. 32 at 59-60); Resnick Dep. at 108:3-110:3 (Ex. UU). They decided that they

1 would be unable to rate sites falling into Fortinet’s Hacking, Phishing, Malware and Spyware
2 categories, and sites falling into the Spam URL classification. See Resnick report at 19-20
3 (Ct. Rec. 32 at 59-60). Thus, Dr. Resnick’s report did not assess FortiGuard’s overblocking
4 rate for Web sites falling into those categories. Id.; see also Resnick Dep. at 49:9-20, 56:18-
5 24 (Ex. UU).

6 Most of the “ratable” URLs were not for full Web pages, but were for so-called
7 “helper images” (1406 URLs) – that is, “little images that are parts of web pages.” See
8 Resnick report at 12-13 (showing examples of embedded images), 20-22 (Ct. Rec. 32 at 52-
9 53, 60-62); Resnick Dep. at 110:4-8 (Ex. UU). As NCRL notes in its paragraph 106, 289
10 URLs were for full Web pages. 194 URLs were for images that Dr. Resnick referred to in his
11 report as “other images.” See Resnick report at 12-13, 20-22 (Ct. Rec. 32 at 52-53, 60-62).
12 Dr. Resnick classified the remaining five URLs as “other.” See Resnick report at 22 (Ct. Rec.
13 32 at 62).

14 According to Dr. Resnick’s study, FortiGuard erroneously blocked 53% (744 of 1,406)
15 of the helper images that it blocked during the week of August 23-29, 2007. See Resnick
16 report at 22-23 (Ct. Rec. 32 at 62-63). Extrapolating from those numbers, FortiGuard
17 erroneously blocks 106 helper images every day on NCRL’s public access computers, and
18 38,688 helper images every year. Moreover, as Dr. Resnick explained in his report:

19 When a policy says that a URL is to be blocked and the destination host returns
20 an image file, instead of passing a blocked message to the patron’s computer,
21 the FortiGate substitutes a small invisible image. This has the advantage of not
22 interfering with the patron’s interaction with other parts of the page from
23 which the embedded image is blocked. The disadvantage, however, is that ...
24 a patron may not realize that anything has been blocked.

25 Resnick report at 12 (Ct. Rec. 32 at 52) (emphasis added); see also Resnick Dep. at 83:19-
26 88:8 (Ex. UU). In other words, FortiGuard blocks embedded images, and erroneously blocks
twice as many such images as it should, without notifying library patrons that the images are
being blocked. In addition, of the 194 blocked full-size images that Dr. Resnick and his

1 colleagues had classified as “other images,” 24 were blocked in error. See Resnick report at
2 23 (Ct. Rec. 32 at 63).

3 With regard to the 289 full Web pages that FortiGuard blocked during the week of
4 August 23-29, 2007, it bears reiterating that NCRL has deployed its filter to block Web sites
5 and not individual Web pages. See Marney Dep. at 93:18-23 (Ct. Rec. 41 at 251); Walters
6 Dep. at 54:11-21 (Ct. Rec. 41 at 298). Thus, with the exception of www.craigslist.org (see
7 Marney Dep. at 102:23-103:14 (Ct. Rec. 41 at 253); Walters Dep. at 53:25-55:18 (Ct. Rec. 41
8 at 298)), if FortiGuard blocks a Web page, it necessarily blocks the entire site of which that
9 page is a part. Dr. Resnick’s study indicates that 289 times every week, NCRL’s FortiGuard
10 filter denies the library’s patrons access to complete Web sites. That means that 41 times
11 every day – 15,028 times every year – an NCRL patron attempts to access a Web site on an
12 NCRL computer and is prevented from doing so by the library’s FortiGuard filter. And this
13 does not include Web sites blocked by FortiGuard under the Hacking, Phishing, Malware and
14 Spyware categories, and under the Spam URL classification.

15 Dr. Resnick’s data also indicate that approximately three times every day, 20 times
16 every week, and 1,040 times every year, an NCRL patron attempts to access a Web site on an
17 NCRL computer and is prevented from doing so because NCRL’s FortiGuard filter has
18 blocked the site in error. And again, these numbers do not include Web sites erroneously
19 blocked under the Spyware, Hacking, Phishing and Malware categories or the Spam URL
20 classification. Thus, the actual number of Web sites that NCRL’s FortiGuard filter
21 erroneously blocks every week is almost certainly larger than 20.

22 36. To clarify Defendant’s Fact #111, see above discussion of Defendant’s Fact
23 #110.

24 37. Defendant’s Fact #113 is inaccurate in several respects. First, as discussed in
25 above with regard to Defendant’s Fact #30, Contrary to Defendant’s Fact #113 FortiGuard
26 was the operative filter at the time several Plaintiffs sought to access a number of Web sites.

1 Second, as Plaintiff Pearl Cherrington testified at deposition, when NCRL’s Internet filter
2 denied her access to an art Web site, she brought the matter to the attention of Terry Dixon,
3 the head librarian at NCRL’s Twisp branch, and was told that Internet access was filtered and
4 that Ms. Dixon was “unable to unlock it.” See Cherrington Dep. at 18:6-13, 20:5-21:11 (Ct.
5 Rec. 41 at 180-81). And third, as Plaintiff Charles Heinlen testified at deposition, in 2004 he
6 asked NCRL staff to unblock a specific “personal Web site,” but his request was denied. See
7 Heinlen Dep. at 31:7-24 (Ct. Rec. 41 at 202). Prior to their respective depositions, neither Ms.
8 Cherrington nor Mr. Heinlen had ever seen a “Material Selection Review Form” – the form
9 that NCRL now claims it made available to patrons so they could request unblocking of
10 specific Web sites. See Cherrington Dep. at 23:2-15 (Ct. Rec. 41 at 181); Heinlen Dep. at
11 30:8-18, 32:9-14 (Ct. Rec. 41 at 202).

12 38. To clarify Defendant’s Fact #115, SAF maintains that
13 www.womenandguns.com was at one time blocked by NCRL’s Internet filter. SAF does not
14 allege that the site is currently blocked.

15 39. To clarify Defendant’s Fact #116, Plaintiff Charles Heinlen attempted to access
16 www.womenandguns.com at NCRL’s Okanogan branch on November 17, 2006. See Heinlen
17 Decl. in Opp. at ¶ 2. NCRL’s filter denied Mr. Heinlen access to that Web site.

18 40. To clarify Defendant’s Fact #119, although www.womenandguns.com may not
19 currently be blocked by NCRL’s FortiGuard filter, Plaintiff The Second Amendment
20 Foundation (“SAF”) is concerned that NCRL will block that Web site (or another site
21 sponsored by SAF) in the future. See Deposition Upon Oral Examination of Alan Merrill
22 Gottlieb (“Gottlieb Dep.”) at 36:25-38:13, 47:12-20 (Ex. PP).

23 41. To clarify Defendant’s Fact #121, Sarah Bradburn primarily patronizes
24 NCRL’s Republic branch. See Bradburn Dep. at 19:14-20:17 (Ct. Rec. 41 at 170);
25 Bradburn’s Discovery Responses, answer to Interrogatory No. 4 (Ct. Rec. 41 at 48).

1 42. Contrary to Defendant's Fact #123, as Ms. Bradburn testified at deposition,
2 although she cannot now recall certain particulars of the incident at NCRL's Republic branch
3 in which she was unable to access information online relating to youth tobacco usage, she
4 believes that NCRL's Internet filter denied her access to that information. See Bradburn's
5 Discovery Responses, answers to Interrogatory Nos. 5, 8 (Ct. Rec. 41 at 48-49); Bradburn
6 Dep. at 18:8-15, 19:14-22:14 (Ct. Rec. 41 at 170-71).

7 43. To clarify Defendant's Fact #126, regardless of whether Ms. Bradburn can
8 recall the specific Web sites to which she was denied access, and although she believes NCRL
9 may employ Internet filtering as its default rule to block certain categories of content, see
10 Bradburn Dep. at 30:2-31:24 (Ex. MM), she wishes to be able to have, on request, unfiltered
11 Internet access for lawful purposes at her local library – something she cannot now have given
12 NCRL's filtering policy. See Bradburn Dep. at 27:17-28:1 (Ex. MM), 35:7-37:11 (Ct. Rec.
13 41 at 172-73).

14 44. To clarify Defendant's Fact #128, Ms. Cherrington primarily patronizes
15 NCRL's Twisp branch. See Cherrington Dep. at 15:12-22, 18:14-22, 20:5-21:4 (Ct. Rec. 41
16 at 179-81); Cherrington's Discovery Responses, answer to Interrogatory No. 4 (Ct. Rec. 41 at
17 60).

18 45. Defendant's Fact #130 is inaccurate. Contrary to Fact #130, although Ms.
19 Cherrington cannot recall some of the specific URLs that she was unable to access because of
20 NCRL's Internet filter, her deposition testimony makes it abundantly clear that the filter
21 denied her access to an Idaho art gallery's Web site and a Web site containing health
22 information. See Cherrington Dep. at 20:5-21:4, 23:16-24:8, 34:16-35:11 (Ct. Rec. 41 at 180-
23 82). In particular, Ms. Cherrington described the blocking screen that the filter displayed
24 when she was denied access to the forbidden Web content. See Cherrington Dep. at 20:5-24,
25 34:16-35:11 (Ct. Rec. 41 at 180, 182). And finally, the head librarian at NCRL's Twisp
26 branch confirmed that the problem Ms. Cherrington was experiencing accessing the art gallery

1 site was caused by the filter. See Cherrington’s Discovery Responses, answer to Interrogatory
2 No. 9 (Ct. Rec. 41 at 62); Cherrington Dep. at 21:3-4 (Ct. Rec. 41 at 180). Ms. Cherrington
3 also stated in her answers to various interrogatories that NCRL propounded, and subsequently
4 testified at deposition, that NCRL’s FortiGuard filter denied her access to YouTube (as noted
5 in NCRL’s paragraph 131). See Cherrington’s Discovery Responses, answer to Interrogatory
6 Nos. 5, 8, 9, 11, 12 (Ct. Rec. 41 at 60-63); Cherrington Dep. at 33:16-34:8 (Ct. Rec. 41 at
7 182).

8 46. To clarify Defendant’s Fact #132, regardless of whether Ms. Cherrington can
9 recall the specific art gallery and health sites to which she was denied access, regardless of
10 whether YouTube is currently unblocked on NCRL’s computer terminals, and although Ms.
11 Cherrington believes NCRL may employ Internet filtering as its default rule to block certain
12 categories of content, see Cherrington Dep. at 25:1-28:21, 40:24-41:11 (Ex. OO), Ms.
13 Cherrington wishes to be able to have, on request, unfiltered Internet access for lawful
14 purposes at her local library – something she cannot now have given NCRL’s filtering policy.
15 See Cherrington Dep. at 24:22-25 (Ex. OO).

16 47. Defendant’s Fact #133 is inaccurate. Contrary to Fact #133, as Ms.
17 Cherrington stated in her answer to NCRL’s Interrogatory No. 9:

18 The denial of access to the art gallery Web sites occurred in early summer
19 2005. On the day access was denied, Ms. Cherrington spoke with librarian
20 Terry Dixon. Ms. Dixon said that the denial of access resulted from the
library’s filtering software and that she was unable to do anything to allow
access to the blocked sites.

21 Cherrington’s Discovery Responses, answer to Interrogatory No. 9 (Ct. Rec. 41 at 62). Ms.
22 Cherrington subsequently testified at deposition that she brought her concerns about her
23 inability to access the Idaho art gallery Web site to the attention of Ms. Dixon, the head
24 librarian at NCRL’s Twisp branch. See Cherrington Dep. at 20:5-21:4 (Ct. Rec. 41 at 180-
25 81).

1 48. Defendant's Fact #134 is incorrect. See discussion of Defendant's Fact #113,
2 Fact #130 and Fact #133 above.

3 49. Contrary to Defendant's Fact #135, NCRL was using FortiGuard when the
4 filter prevented Ms. Cherrington from accessing YouTube. See ¶¶ 113 and 130 above; see
5 also Cherrington's Discovery Responses, answers to Interrogatory Nos. 5, 8, 9, 11, 12 (Ct.
6 Rec. 41 at 60-63).

7 50. To clarify Defendant's Fact #137, Mr. Heinlen has also patronized NCRL's
8 Moses Lake, Tonasket and Oroville branches. See Heinlen's Discovery Responses, answer to
9 Interrogatory No. 4 (Ct. Rec. 41 at 72).

10 51. Defendant's Fact #139 is incorrect. See discussion of Defendant's Fact #113,
11 Fact #130 and Fact #133 above.

12 52. To clarify Defendant's Fact #141, although Mr. Heinlen does believe he should
13 have access to the types of online materials referenced in this paragraph (as he testified at
14 deposition, "[u]nblocked is unblocked," Heinlen Dep. at 51:13; see also id. at 38:4-40:7,
15 44:13-47:6, 54:19-25 (Ex. QQ)), he did not testify that he believes he or any other NCRL
16 patron has a right to actually view materials that are not protected by the United States or
17 Washington State Constitutions. To the contrary, he testified at deposition that he does not
18 wish to look at pornography or engage in illegal activity on NCRL's computers, id. at 26:14-
19 25 (Ct. Rec. 41 at 201) ("I'm trying to lawfully surf the Net on a library terminal.... I'm not
20 looking for any X-rated sites or anything."), 38:4-12 (Ct. Rec. 41 at 204), 46:20-22 (Ex. QQ);
21 and that if any patron were to perform an illegal act on library property, NCRL would be
22 "well within [its] rights to get the police right across the street and deal with it accordingly,"
23 id. at 44:13-23 (Ex. QQ).

24 Mr. Heinlen does, however, wish to be able to have, on request, unfiltered Internet
25 access for lawful purposes at his local library – something he cannot now have given NCRL's
26 filtering policy. See Heinlen Dep. at 38:4-7, 46:16-18, 52:20-53:7, 54:19-25 (Ex. QQ).

1 52. Contrary to Defendant’s Fact #142, Plaintiffs filed their Complaint for
2 Declaratory and Injunctive Relief (“Complaint”) in this matter on November 16, 2006. Ct.
3 Rec. 1.

4 54. Contrary to Defendant’s Fact #143, NCRL answered Plaintiffs’ Complaint on
5 January 2, 2007. Ct. Rec. 5.

6 55. Contrary to Defendant’s Fact #146, NCRL’s Answer and Affirmative Defenses
7 (“Answer”) merely asserted that “Plaintiffs have failed to allege facts constituting a present
8 case or controversy.” Ct. Rec. 5 at 5. The Answer did not explain the grounds for that
9 assertion. Id. In any event, NCRL has not come forward with any evidence to support its
10 suggestion that all the specific Web sites to which Plaintiffs were previously denied access
11 have been unblocked.

12 56. Plaintiffs object to Defendant’s Fact #149 because it is predicated on
13 declaration testimony by Thomas Adams that is hearsay and is not based on personal
14 knowledge, and on a hearsay exhibit (Ex. G) to Mr. Adams’ declaration. Should the Court
15 decide to consider NCRL’s Fact #149 and the declaration testimony and exhibit on which it is
16 based, however, the Court should also consider the following information pertaining to the
17 lawsuit referenced in Fact #149 and in the corresponding exhibit to Mr. Adams’ declaration:

18 Attached hereto as Exhibit HHH is a copy of the complaint that was filed in Adamson
19 v. Minneapolis Public Library, No. 03-02521 (D. Minn. March 24, 2003) (“Adamson
20 Complaint”), the case referenced in NCRL’s Fact #149. In Adamson a group of librarians
21 challenged a library policy that expressly allowed patrons to view obscenity on library
22 computers, and instructed library staff not to intervene if a user viewed obscenity and even if
23 the user invited minors to view obscenity with them. See Adamson Complaint at ¶¶ 26-29,
24 38-41, 44-45. According to the Adamson Complaint,

25 [Library administrators] made no effort to limit the viewing of legally obscene
26 material on its terminals. They put no limits on the amount or type of material
patrons could print out on MPL printers. They took no steps to prevent
children from viewing obscene and pornographic materials at the library. They

1 specifically directed their security staff not to respond to staff requests to cause
2 patrons to stop viewing these materials. They did not remove patrons who
3 behaved inappropriately towards staff or other patrons except in the most
4 extreme circumstances and even then only for short periods of time. At no
time did MPL provide any training to its managers or supervisors on how to
deal with the hostile and offensive working environment created by library's
policy of unfettered Internet access.

5 ¶ 60.

6 Attached hereto as Exhibit III is a copy of the U.S. District Court's docket sheet in
7 Adamson. It indicates that the parties to the lawsuit settled their dispute, and that the case was
8 dismissed on August 28, 2003 without any court ruling on the merits.

9 Attached hereto as Exhibit JJJ is a copy of the Minneapolis Public Library's current
10 Internet use policy, which was downloaded from the Web site
11 <http://www.mpls.lib.mn.us/policy.asp> on February 14, 2008. The library's policy indicates
12 that it was revised effective August 25, 2004, in the wake of the Adamson settlement. (The
13 Web site has the logo of the Hennepin County Library on it because the Minneapolis Public
14 Library merged with the Hennepin County Library effective January 1, 2008. As indicated in
15 the text of the policy, this exhibit reflects the policy of the Minneapolis Public Library from
16 the time of adoption to the present.) The stated policy of the Minneapolis library currently
17 includes the following language:

18 The [Minneapolis Public] Library upholds and affirms the right of every
19 individual to have access to constitutionally protected material on the Internet.
20 The content of the Internet is not managed or governed by any entity, therefore
users may encounter materials they consider offensive.... Parents and
guardians are responsible for monitoring Internet access by children.

21 The Children's Internet Protection Act (CIPA), passed by Congress in 2000
22 and upheld by the Supreme Court in 2003, requires libraries receiving certain
23 types of federal funding to equip Internet-access computers with a technology
24 protection measure that blocks or filters visual depictions that are obscene,
25 contain child pornography or are harmful to minors. In compliance with CIPA,
26 the Library Board authorized installation of filtering software designed to
prevent access to obscenity, child pornography and materials harmful to
minors. In accordance with the law, persons aged 17 years or older may
request to have the filters disabled for any lawful purpose that meets the
Minneapolis Public Library Internet Policy and Guidelines AND THE FILTER
WILL BE DISABLED.

1 ... Illegal use of the Internet is prohibited. Library users may not use the
2 Library's Internet access to view, print, distribute, display, send or receive
3 images, text or graphics of obscene material or material that violates laws
relating to child pornography. Library users may not disseminate, exhibit or
display to minors materials that are harmful to minors.

4 57. Plaintiffs object to Defendant's Fact #150 because it is predicated on
5 declaration testimony by Thomas Adams that is hearsay and not based on personal
6 knowledge, and on a hearsay exhibit to Mr. Adams' declaration. Should the Court decide to
7 consider Defendant's Fact #150 and the declaration testimony and exhibit on which it is
8 predicated, however, the Court should also consider that, based on the newspaper article cited
9 by NCRL, all Internet access on the Dallas library system's public computer terminals is
10 unfiltered at all times – both for adults and for children. Ct. Rec. 30 at 50-51. Here, by
11 contrast, Plaintiffs merely seek an order that would require NCRL to disable its FortiGuard
12 filter at the request of adults who wish to use the Internet for bona fide research or other
13 lawful purposes. The Court should also consider the fact that an urban library system like the
14 one in Dallas is likely to have a very different clientele than a rural library district in a five-
15 county region like the one Dean Marney described as follows during his deposition:

16 Q. What is it about this community that would make it likely to support a
17 policy of filtering all computers all the time?

18 A. An example would be within five counties, to my knowledge there's only
19 one adult book store. There are no stripper bars in five counties. There's
an expectation that we're – that we go for the best.

20 Q. The best being –

21 A. There is – there is an expectation that we have that we support cultural
things that are traditional.

22 Q. Can you give me some examples?

23 A. There's an expectation that we have Jane Austen on the shelves whether
24 people read it or not.

25 Marney Dep. at 102:4-15 (Ct. Rec. 41 at 253).

26 Much more similar to NCRL than the Dallas library system are the Stark County
District Library ("SCDL"), headquartered in Canton, Ohio; the Fairbanks North Star Borough

1 Library in Fairbanks, Alaska (“FNSBL”); and the Jefferson County Library District (“JCLD”)
2 in Madras, Oregon. See Deposition of Kenton Oliver (“Oliver Dep.”) at 12:24-13:8, 36:20-
3 41:13 (Ex. SS); Deposition Upon Oral Examination of June Pinnell-Stephens (“Pinnell-
4 Stephens Dep.”) at 6:25-10:16, 16:20-22:1, 27:23-29:20 (Ex. TT); Deposition of Sally W.
5 Beesley (“Beesley Dep.”) at 14:19-21:25 (Ex. LL). These library systems are more rural in
6 nature, and include very small branch libraries similar to several of NCRL’s branches. Id. As
7 noted in Plaintiffs’ Statement of Facts in Support of Their Motion for Summary Judgment, at
8 ¶¶ 120-31, these libraries either do not filter Web content (JCLD) or disable the filter at the
9 request of adults (SCDL and FNSBL), and they have not experienced problems with
10 excessive viewing of pornography by library patrons.

11 DATED this 25th day of February, 2008.

12 AMERICAN CIVIL LIBERTIES UNION OF
13 WASHINGTON FOUNDATION

14 By: /s/ Aaron H. Caplan

15 Aaron H. Caplan, WSBA #22525
16 American Civil Liberties Union of Washington
17 Foundation
18 705 Second Avenue, Third Floor
19 Seattle, WA 98103
20 Tel. (206) 624-2184
21 Fax (206) 624-2190
22 caplan@aclu-wa.org

23 Duncan Manville, WSBA #30304
24 1629 2nd Avenue W.
25 Seattle, WA 98119
26 Tel. (206) 288-9330
27 Fax (206) 624-2190
28 duncan.manville@yahoo.com

29 Catherine Crump, pro hac vice
30 American Civil Liberties Union Foundation
31 125 Broad Street, 18th Floor
32 New York, NY 10004
33 Tel. (212) 519-7806
34 ccrump@aclu.org

35 Counsel for Plaintiffs

1 **CERTIFICATE OF SERVICE**

2 I hereby certify that on February 25, 2008, I electronically filed the foregoing
3 document with the Clerk of Court using the CM/ECF system, which will send notification of
4 such filing to the persons listed below:

5 Thomas D. Adams
6 Celeste Mountain Monroe
7 KARR TUTTLE CAMPBELL
8 1201 Third Avenue, Suite 2900
9 Seattle, WA 98101

Attorneys for Defendant

DATED this 25th day of February, 2008.

10 AMERICAN CIVIL LIBERTIES UNION OF
11 WASHINGTON FOUNDATION

12
13 By: /s/ Aaron H. Caplan
14 Aaron H. Caplan, WSBA #22525
15 American Civil Liberties Union of Washington
16 Foundation
17 705 Second Avenue, Third Floor
18 Seattle, WA 98103
19 Tel. (206) 624-2184
20 Fax (206) 624-2190
21 caplan@aclu-wa.org
22
23
24
25
26