

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	
THE AUTHORS GUILD, INC., et al.,	:
	:
Plaintiffs,	:
	:
- against -	:
	:
HATHITRUST, et al.,	:
	:
Defendants.	:
	:
-----X	

Index No. 11 Civ. 6351 (HB)

DECLARATION OF BENJAMIN EDELMAN

I, Benjamin Edelman, hereby declare as follows:

Introduction and Qualifications

1. I am an assistant professor at Harvard Business School. My research focuses on the design of electronic marketplaces, including Internet advertising, search engines, privacy, and information security. I hold a Ph.D. in Economics from Harvard University, a J.D. from Harvard Law School, an A.M. in statistics from Harvard University, and an A.B. in economics from Harvard College. Further information concerning my background and qualifications is provided in my curriculum vitae, which is attached hereto as Exhibit A.

2. My experience includes more than 15 years as a computer programmer, during which time I developed software for my own use, as well as for end-user computers, local networks, and web servers. I also administered servers for myself and others. My technical experience includes efforts to verify the security of other programmers' code, including uncovering shortfalls in their security systems. I have studied and written about issues of information security, accidental information revelation, and information distributed more broadly than online services anticipated. For example, I have uncovered multiple privacy flaws in

connection with services provided by Google, Inc. (“Google”), including improper data collection by Google Toolbar as well as improper data distribution by Google JotSpot. I also found and demonstrated to a court’s satisfaction that an early online video service, iCraveTV, had failed to secure video contents in the way that it had previously represented to that court.

3. My academic publications explore a variety of aspects of online business, including multiple articles considering the difficulty of limiting access to and use of information systems. A full list of my publications is provided in my curriculum vitae (Exhibit A). Among the publications relevant to questions at issue in this matter are the following articles:

Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, a submission to Industry Canada in which I evaluated the difficulty of imposing certain access restrictions when distributing video material over the Internet and *Securing Online Advertising: Rustlers and Sheriffs in the New Wild West*; in which I presented the challenges of designing online advertising markets to satisfy the requirements of advertisers, online publishers, and advertising platforms while unauthorized activities such as advertising fraud are taking place. In numerous articles, I have described all manner of online miscreants using information systems in ways their providers did not intend, did not anticipate, sought to prevent, and/or claimed to seek to prevent.

4. My teaching assignment currently consists of a Harvard Business School elective course called *The Online Economy*, which analyzes strategies for all manner of online businesses. Among other topics, this course addresses issues of information security.

5. I have testified as an expert witness in federal and state courts including in the U.S. District Courts for Michigan and Pennsylvania and in Utah State Court. I also served as an expert for the plaintiffs in the so-called “Google Books” case that also is pending in this District. *Authors Guild v. Google, Inc.*, 05 Civ. 8136 (DC). That case presents many of the same facts

and concerns as are raised by this case. A listing of the other cases in which I have testified as an expert at trial or by deposition during the past four years is attached as Exhibit B. I also have testified before committees of the United States House of Representative and United States Senate.

6. I am being compensated for my work in this matter at the rate of \$450 per hour.

Scope of Retention

7. My understanding is that the Plaintiffs in this case have commenced a lawsuit against certain universities as well as the HathiTrust (collectively, the “Defendants”) alleging that these Defendants have collaborated with Google to digitally scan more than ten million printed books from university libraries, including millions of books that still are protected by copyright (the “Google Library Project”). My further understanding is that Google has retained a digital copy of each of these books, and that Defendants have received their own digital copies of the printed books they provided to Google, which they then copied and incorporated into the HathiTrust Digital Library (“HDL”), which comprises multiple server farms and backup tapes. As described below, Defendants have used, or threatened to use, these digitized works in a number of ways.

8. In this report, I address and opine on risks of a security breach exposing widely online the contents of in-copyright books that have been digitized as part of the Google Library Project. I conclude that Defendants’ storage and use of the digital book copies creates a significant security risk which threatens to cause a substantially adverse impact on the market for the books.

9. If Defendants’ conduct is found to be a fair use and Defendants are permitted to continue storing and using digital copies of copyrighted works in their shared digital repository, there will be serious risks of digital piracy, notwithstanding the access limitations and security

controls Defendants have established. The risks will increase substantially if a precedent set in this case that would permit persons or entities with weaker security controls to provide even limited access to digital versions of copyrighted works.

10. In preparing this report, I have reviewed the First Amended Complaint filed by Plaintiffs, the Answer to the First Amended Complaint filed by Defendants, and the motion papers filed by both sides in connection with Plaintiffs' motion for partial judgment on the pleadings. In addition, I have reviewed the sources described in this declaration as well as the additional materials listed on Exhibit C.

Piracy of Books is Already a Real, Not Hypothetical Problem

11. The electronic of digital copies of books, without authorization from publishers or rights-holders, is already occurring. For example, consider a user seeking a copy of *Calico Joe*, by John Grisham, which is the number one bestseller hardcover fiction book according to the New York Times bestseller list dated July 1, 2012. Such a user might run a Google search for "calico joe mobi" (without quotes), using the word "mobi" to indicate interest in a ".mobi" book (a popular electronic book file format). Each and every one of the first ten links found from that Google search offer or purport to offer copies of *Calico Joe*. I checked each of these ten links and found that eight confirmed that the book was available and offered a download link or download instructions. Of the ten links, not one pointed to a site that charged for access to the book. Given that *Calico Joe* is a top-selling in-copyright commercial publication one can be virtually certain that this offering of free electronic copies is being made without permission from the copyright holder or his publisher.

12. Sites offering pirated books fall into several categories. Some sites charge for pirated book copies, though they do not share the resulting revenues with those who created the books. Other sites distribute pirated book copies for free. Among sites offering free book

copies, some offer direct web-based downloads, providing pirated book copies when a user simply clicks to request a copy. Other sites offer links to Bit torrent “.torrent” files that direct a user’s computer to other computers from which a desired file may be copied.

13. A site variously known as library.nu, ebooksclub.org and gigapedia.com (collectively referred to below as “library.nu”) has facilitated particularly widespread unauthorized copying of books. According to a legal complaint from publishers, library.nu provided access to 400,000 electronic books. While library.nu was shut down pursuant to court order, the actions of library.nu continue to harm the market for books. In a presentation entitled *Media Piracy in Emerging Cultures*, Joe Karaganis, whose work at Columbia University focuses on the relationship between digital convergence and cultural production, and has recently included research on broadband adoption, data policy, and media piracy, explained the phenomenon of “shadow libraries” like library.nu as follows:

As cheap digital technologies displace paper, we’re seeing the emergence of something new: Massive digital copying, and in particular. the building, sharing and curation of large-scale digital archives among students, researchers and bibliophiles. . . . with students in the lead. And they’re just not waiting for the resolution of the larger legal questions around these issues. Not the orphan works issue, not the digital library lending model issue, the academic licensing issue, the Google Books settlement issue. They’re just doing it.

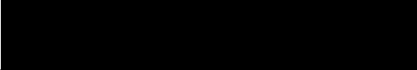
Joe Karaganis, *Media Piracy in Emerging Cultures*, audio and presentation available at <http://www.law.berkeley.edu/11731.htm> (April 13, 2012).

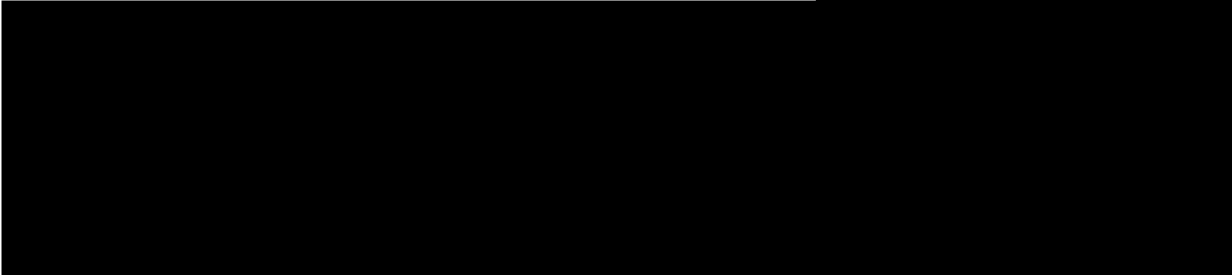
14. In my experience as a student and professor, I have personally observed first-hand the emergence and existence of such shadow libraries containing “free” digital copies of textbooks and other works, even after the demise of library.nu. Once electronic books have been placed into widespread circulation, such as what happened with library.nu, it is very difficult to prevent those files from continuing to circulate among anyone interested.

The Digital Books Stored and Used by Defendants are Exposed to Numerous Risks

15. If Defendants, Google or other providers (“providers”) scan books, the resulting digital book copies could enter widespread public circulation via any of several channels.

16. *First*, pirates could extract book copies through defects in the security of a provider’s systems. Once books are scanned, the resulting digital files are stored on a server or, more often, multiple servers. Based on the documents I have reviewed, the HDL employs two synchronized server farms, including a primary site in Ann Arbor and a mirror site in Indianapolis, as well as two separately-located sets of backup tapes, all of which are connected to a campus network (which presumably is connected to the Internet). Defects in the physical or virtual access controls of any such server or access point could allow pirates to gain access to digital book copies. Defects could also arise through flaws in the operating system, database server, web server, or other software run on a provider’s servers; such flaws have been widespread in even the most popular server software. Moreover, defects could also arise through the provider’s custom software, which is likely to be less secure because custom software usually receives a lesser level of scrutiny, testing, and verification than software that is distributed and used more broadly. I understand that the HDL server farms include web and database servers connected to the Internet, posing additional risks.

17. *Second*, pirates could extract books via errors in the security configuration of a provider’s systems. If even one of a provider’s servers lacks a required update or other security feature, pirates could use that server to obtain the book copies. 



18. *Third*, a rogue employee could intentionally redistribute book copies. Rogue employees gain and exploit privileged access to data despite organizations' efforts to screen and supervise key staff. Consider the classified U.S. State Department material distributed by Wikileaks in 2010 – information obtained via a rogue employee. A rogue employee with access to book copies could intentionally make those copies available to the public. HathiTrust's Response to Plaintiffs' First Set of Interrogatories confirms that numerous employees enjoy authorized access to HDL book copies. Specifically, HathiTrust Response No. 2(1) identifies six employees with physical access to the server farm in Ann Arbor, three employees with physical access to the server farm in Indianapolis, five employees with physical access (and six employees with virtual access) to the two sets of backup tapes in Ann Arbor and ninety-three employees, students and faculty with virtual access to the copyrighted digital files stored on the primary and mirror HathiTrust servers. Any of these individuals could intentionally download and redistribute book copies.

19. *Fourth*, pirates could extract books by impersonating provider staff to access provider systems, including impersonating any of the twenty authorized persons noted in HathiTrust interrogatory response 2.1. Suppose an attacker can obtain the username and password of a person with full access to a provider's book copies. The attacker can log in with that password to access and copy the provider's book copies. Similar attacks are frequent: For example Amazon Zappos,¹ Gawker,² and Microsoft Hotmail³ suffered this type of attack in

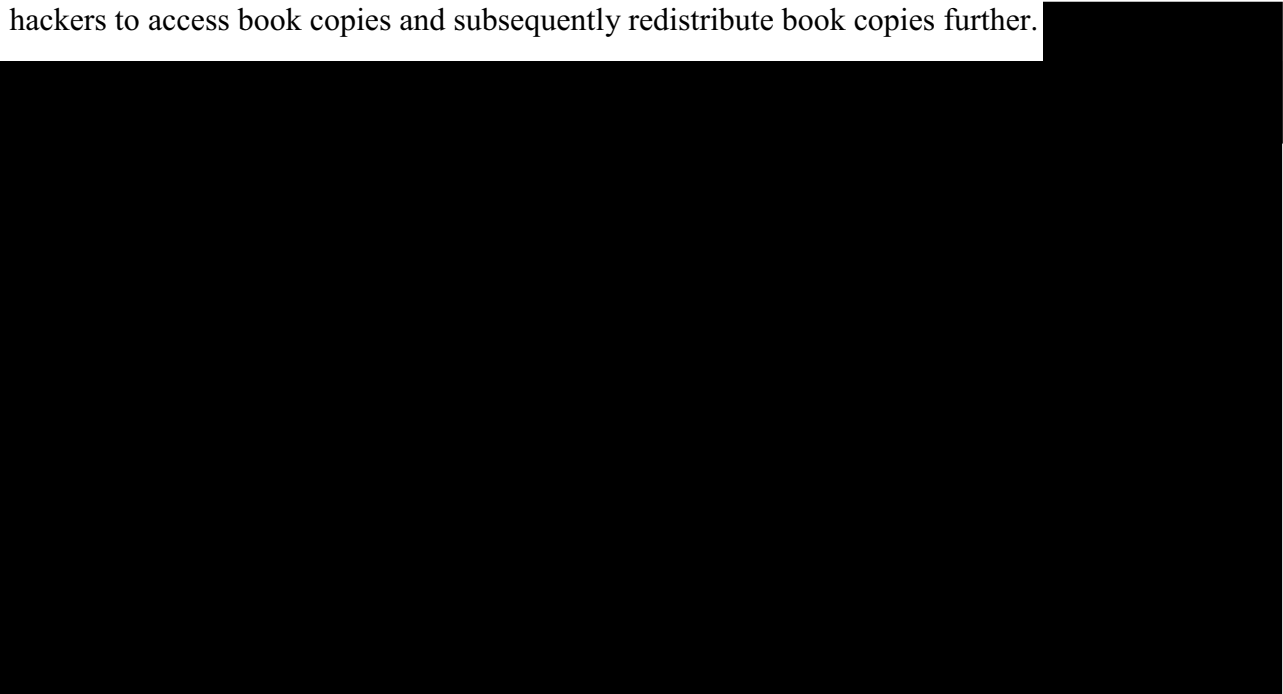
¹ Dominic Rushe. "Zappos Database Hit by Cyberattack." The Guardian. January 16, 2012.

² Zachary Seward and Albert Sun. "The Top 50 Gawker Media Passwords." Wall Street Journal - Digits. December 13, 2010.

³ Bogdan Calin. "Statistics from 10,000 Leaked Hotmail Passwords." Acunetix. October 6, 2009. <http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/>.

2009-2011. Even the United Nations has suffered a breach of a similar nature.⁴ If a single staff person at a single book provider used the same password for a hacked site and for access to book copies, then a hacker could use that password to access book copies, copy book copies to the hacker's own systems, and redistribute book copies further from there.

20. *Fifth*, any error made by any employer could create a security breach allowing hackers to access book copies and subsequently redistribute book copies further.

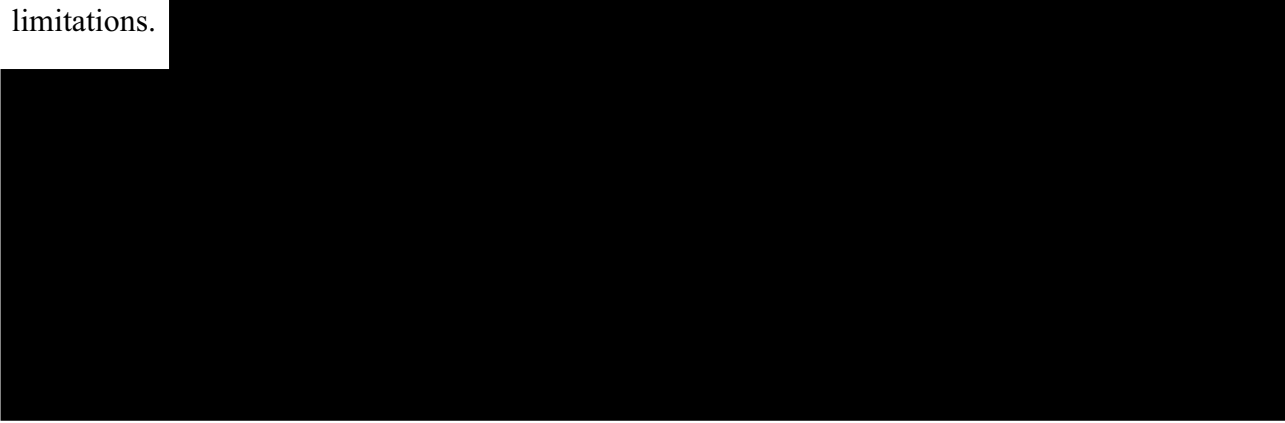


21. *Sixth*, if providers allow privileged access to copyrighted book content, it is likely that some users will attempt to exceed the intended scope of authorization to access and copy book contents en masse. I have not been fully informed of all the ways that Defendants intend to use the book contents data they receive from Google, nor have I been informed how they intend to secure that data. But the information I have reviewed indicates that Defendants' actions present a risk of book piracy. My understanding is that Defendants intended to display digital copies of entire books that they considered to be "Orphan Works" (i.e., works whose copyright

⁴ Chloe Albanesius. "Team Poison Hacks UN, Leaks Usernames, Passwords." PC Magazine. November 30, 2011.

owner could not easily be found), but suspended that program in the face of this lawsuit. I also understand that Defendants make digital copies of certain works available as replacements for physical books in their collections designated as damaged or deteriorating, as well as under specific conditions to visually-disabled students. As noted above in Paragraph 18, at least ninety-three people located throughout the country are granted “privileged” access to view, download and print all the books in the HDL. *See Wilkin Tr. 192:11-194:13* (testifying that users authenticated with “privileged” access can view, download and print any work in the HDL).

22. Even if Defendants attempt to implement security controls and other limitations on users’ ability to download book copies, experience suggests that users will exceed those limitations.



23. I understand that Defendants are also using the massive digital corpus to allow certain users to conduct so-called “non-consumptive research,” including analyzing word and phrase usage and patterns in book text. From the perspective of a researcher seeking to perform such analysis, it is natural to begin by copying digital book copies onto a computer system the researcher controls, allowing the researcher to run flexible and high-speed searches of those book copies using the researcher’s preferred tools. (In contrast, if the researcher had to run analyses on a server controlled by the library, the researcher would ordinarily be able to use only those tools the library provides, and the speed of the researcher’s analysis might be constrained by

server capacity and availability.) Crucially, once a researcher copies the data onto his own system, the library's prior security efforts (whatever they might be) become largely irrelevant. A researcher might even store digital book copies on a laptop or USB drive, which are particularly susceptible to loss and theft. When book copies are processed into text using optical character recognition, the resulting files can be quite small – making it feasible to store tens of thousands of book copies on an ordinary laptop or USB drive.

24. A striking example of an authorized user exceeding the intended level of access to download mass quantities of library materials involves the case of Aaron Swartz, an internet activist and co-founder of Demand Progress, a political action group that has, among other things, supported Wikileaks. In July 2011 Swartz was indicted after, according to the indictment breaking into a restricted area at MIT and entering a computer wiring closet, supplying false information to bypass security measures and downloading over four million articles and other copyrighted documents.⁵

25. *Seventh*, when books are scanned by a smaller and less sophisticated provider, there is a particularly acute risk of book contents being accessed and redistributed. For one, less sophisticated organizations have a reduced capability to design, install, and maintain suitable web site, database, and related security systems as well as anti-reconstruction systems to secure books. Furthermore, less sophisticated organizations have a lesser ability to screen key staff to prevent data loss through rogue employees, and a lesser ability to configure security systems to exclude hackers. Thus, if Defendants' conduct is found to be legal, and if other companies and organizations follow Defendants' lead in scanning books, the risk that book contents will be accessed and redistributed becomes even greater.

⁵ *United States of America v. Aaron Swartz*. Indictment. July 14, 2011.

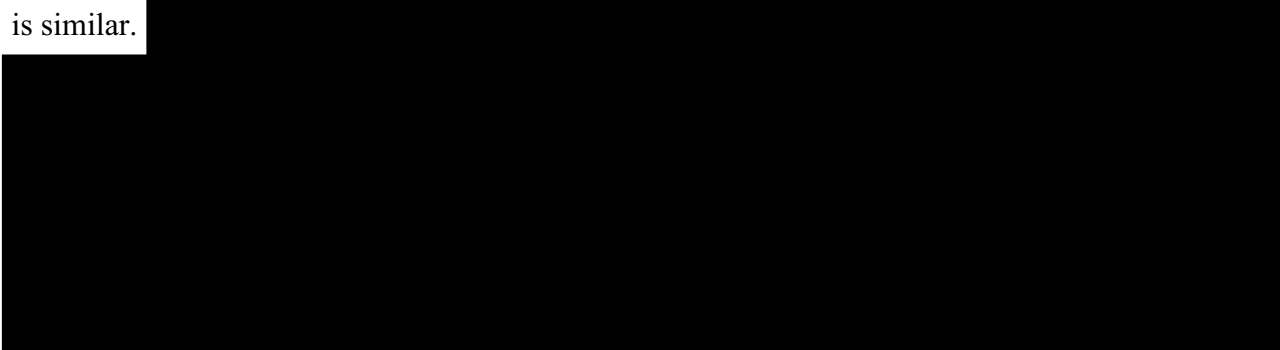
26. As set out in the section of this report captioned “A Single Breach Could Cause Devastating Harm,” one instance of book copying can have large effects. For example, if numerous companies and organizations scan books, attackers can focus their efforts on whichever installs the weakest security. Similarly, attackers can take advantage of even a brief period when a single book provider is insecure (for example, through failure to properly update a server). Once attackers obtain book copies, they can then redistribute the copies as desired. If many providers begin scanning and storing digital book copies, the affected books are only as secure as the least secure provider – so the diligent efforts of some providers would be undermined by lax security of others.

27. Some rightsholders may be willing to accept these risks in order to obtain the benefits of online distribution of their works. Other rightsholders may be willing to accept these risks only if they are appropriately compensated for the risk of piracy, for example if they receive contractual guarantees as to the steps to be taken to mitigate that risk, or if they receive appropriate compensation if piracy occurs. If large-scale book scanning requires permission from rightsholders, rightsholders will be able to express these preferences and obtain corresponding protections for their works. Conversely, if such scanning is deemed permissible without permission from rightsholders, then rightsholders will have little or no means to reduce risks they consider gravely important.

Factors Unique to Academic Institutions Raise the Risk

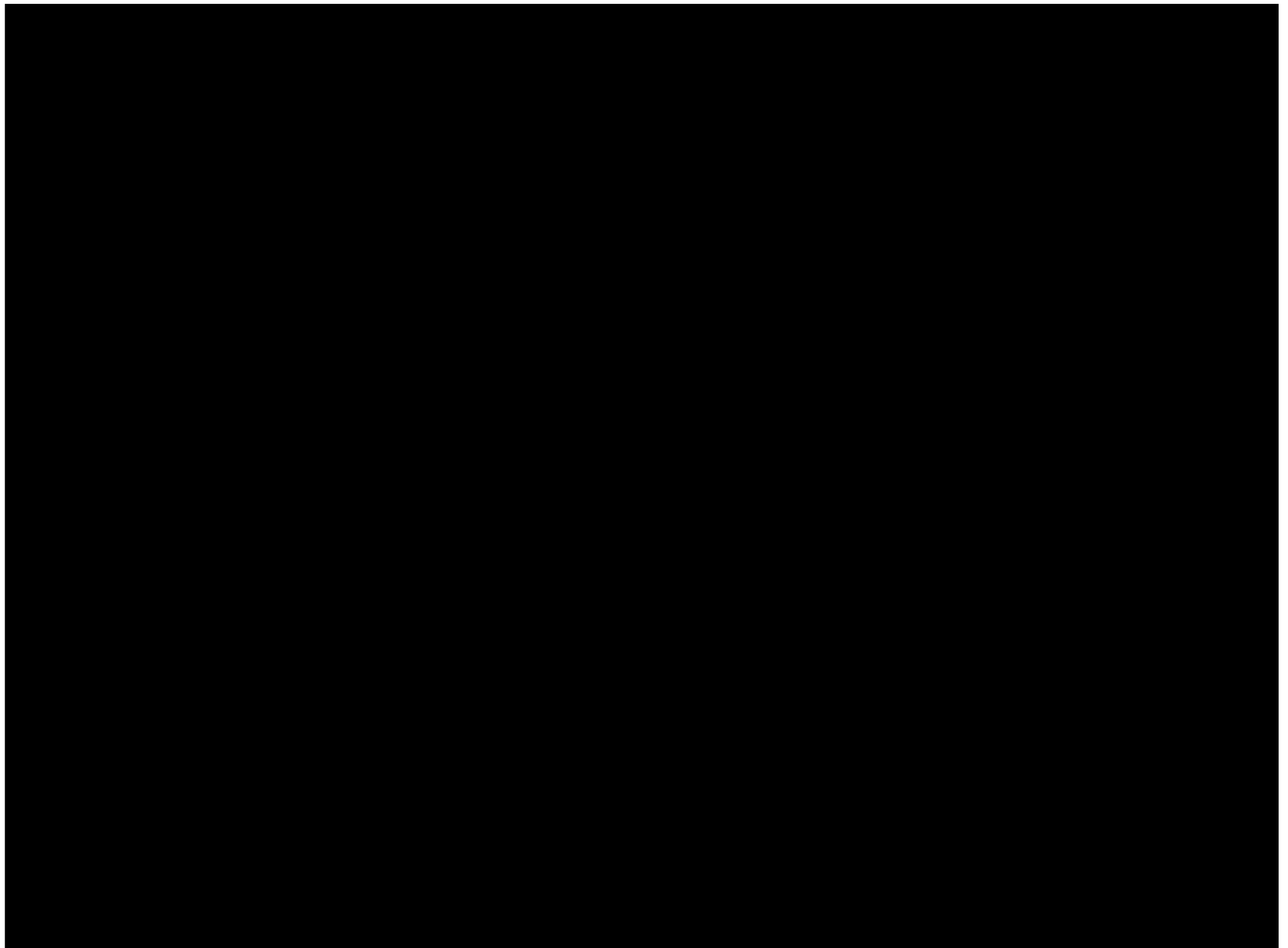
28. Structural factors unique to the academic setting also increase the difficulty of libraries properly securing book contents. University libraries typically serve myriad users including students, visitors, and others with limited long-term connection to the library – limiting a library’s ability to establish accountability. Moreover, libraries typically specialize in making information available rather than in restricting how information may be used.

29. While some libraries offer electronic resources that are subject to restrictions on use, these restrictions are typically implemented by keeping the information on the information provider's servers so that the information provider, not the library, can monitor usage and attempt to assure compliance. For example, when libraries license journals and articles and other documents from the JSTOR digital archive, they generally do not receive full copies of the articles to store on library servers. Instead, libraries receive secure access to JSTOR servers, allowing library patrons to access individual documents on JSTOR without ever receiving the full corpus of all articles JSTOR holds. Access to documents held by Lexis-Nexis and Westlaw is similar.



30. From my time on university campuses, both as a student and as a faculty member, I am familiar with the views held by many students and some faculty with respect to copyright law. Many such users view it as permissible to make copies of all manner of copyrighted content. Often, receiving materials in digital form seems to embolden users: I know many people who would never steal an item from a retail store and who hesitate to photocopy a book (whether because such photocopying is too time-consuming, or because it "feels wrong" to them), but who do not hesitate to make copies of copyrighted works using tools such as BitTorrent or, before they were shut down, Napster and Kazaa. The prevalence of these views on university campuses makes it particularly likely that copying digital books, from university libraries or otherwise, would be seen as ethically acceptable.

31. A further risk of book piracy from or via university libraries comes from the culture of “pranks” enjoyed by many software and engineering students. For example, the MIT Hack Gallery presents hundreds of hacks including public displays of the Apple logo, the logo of the Boston Red Sox, and the logos of various movies.⁶

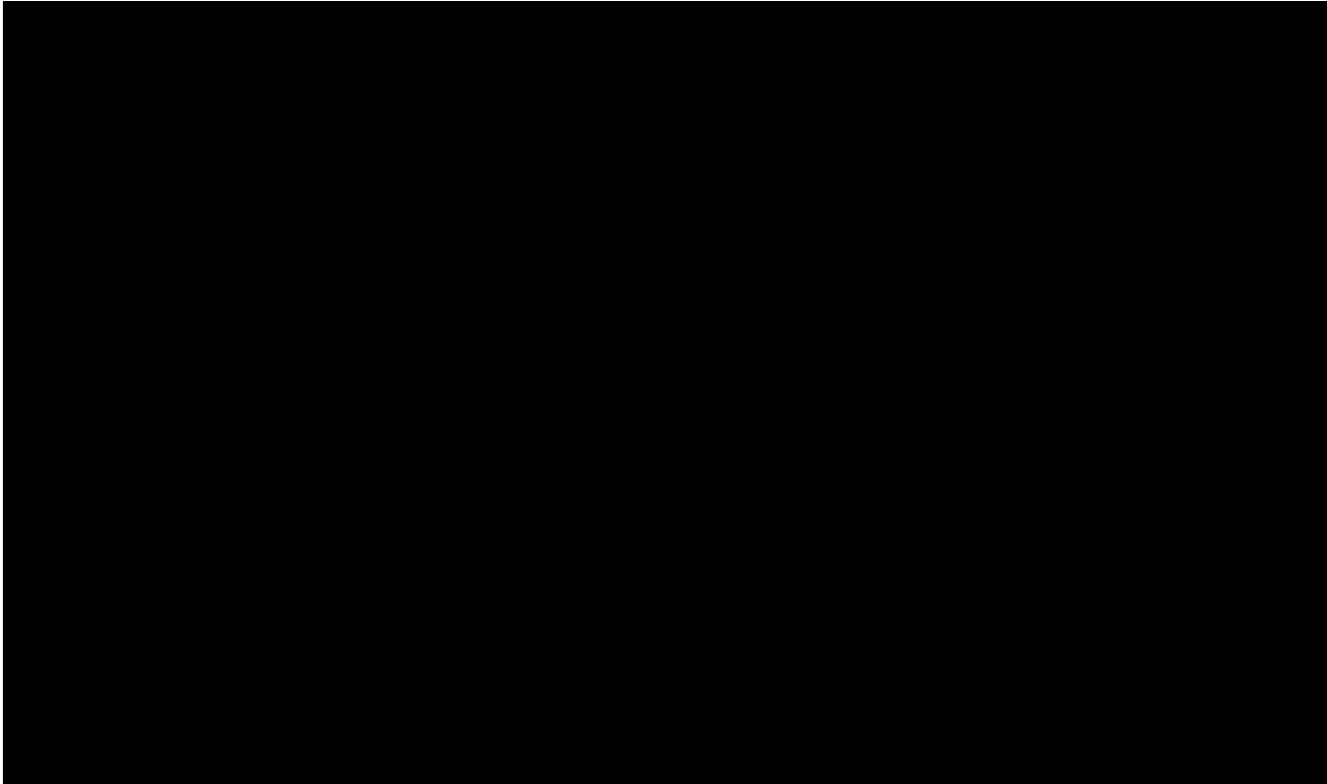


⁶ <http://hacks.mit.edu/>.

⁷ Cooperative Agreement between Google Inc. and Regents of the University of Michigan, sections 2.3.1 and 2.7.

⁸ Cooperative Agreement between Google Inc. and Regents of the University of Michigan, sections 4.4.1-2.

⁹ For example, the Google NDA presented at <http://valleywag.com/230407/this-nda-never-existed> offers greater protection including greater restrictions on the circumstances in which



Google Itself Is Not Immune to Design Flaws and Security Breaches

34. Despite Google’s considerable resources, Google products and services nonetheless suffer from design flaws and security breaches which result in information flowing in ways Google and/or users did not intend.

35. In general, Google faces each of the vulnerabilities detailed in the section entitled “Similar Scanning Operations Could Allow Book Copies to Be Copied and Redistributed” above. The following sections flag specific problems that could occur, as well as noting similar problems Google has already faced.

Google’s Security Systems are not Failproof

36. In other information and distribution services, Google has failed to comply with its commitments to users and the public. For example, in January 2010, I found and reported the

information can be shared, greater restrictions on the permissible recipients of such information, and more precise requirements as to how information must be secured.

popular Google Toolbar program – installed on “hundreds of millions” of computers¹⁰ – continuing to track users’ browsing (including every web page visited) even after users had specifically requested that the Toolbar be “disable[d]” and even after the Toolbar had confirmed users’ request and disappeared from screen.¹¹ The user browsing at issue was users’ most sensitive online activities: reasonable users would activate the Toolbar’s “disable tracking” feature exactly when they sought to engage in private activities they did not wish Google to track. Google subsequently characterized its nonconsensual information collection as “an issue”¹² but offered no explanation for why it collected information users had specifically indicated, and Google had agreed, should not be collected. Google has paid no compensation to affected users. Neither did Google promise to undo the error: Google never offered to let affected users identify themselves so Google could delete their data from its records.

37. In early 2010, Google introduced Buzz, a social network for connecting to online colleagues and sharing information about who is doing what. For users of Google’s email service, Gmail, Buzz shared with the general public the names of the persons Gmail users corresponded with – information Google had previously indicated it would keep confidential. Google subsequently faced class litigation for this information breach, alleging that affected users suffered direct economic loss as a result of Google’s information revelation. For example,

¹⁰ Ian Paul. “Google Toolbar Tracks Some Browsing Even When It’s Not Supposed To.” PC World. January 25, 2010. http://www.peworld.com/article/187670/google_toolbar_tracks_some_browsing_even_when_its_not_supposed_to.html .

¹¹ Benjamin Edelman. “Google Toolbar Tracks Browsing Even After Users Choose ‘Disable’.” January 26, 2010. <http://www.benedelman.org/news/012610-1.html> .

¹² Barry Schwarz. “Disabling The Google Toolbar Doesn’t Stop Google From Tracking You.” January 26, 2010. <http://searchengineland.com/disabling-the-google-toolbar-doesnt-stop-google-from-tracking-you-34438>

Buzz revealed the persons sending email to and receiving email from Andrew McLaughlin, who had previously served as a Google lobbyist, and was working in the White House as deputy Chief Technology Officer of the United States. Buzz's information revelation indicated that Mr. McLaughlin had engaged in impermissible activities with his prior employers, in violation of White House ethics rules. After Buzz-posted information prompted a complaint and an investigation, Mr. McLaughlin was formally reprimanded for the improper communications.¹³ To the best of my knowledge, Google never offered any compensation to Mr. McLaughlin or other affected Gmail users.

38. In addition, during February 2012, researchers discovered that Google was bypassing Safari and Internet Explorer privacy settings to collect data that those browsers would ordinarily decline to provide.¹⁴ While Google ceased further collection via these methods, Google has not offered to delete information improperly collected, nor has Google offered to compensate affected users.

39. In each of these examples, Google's services worked in exactly the way Google's engineers designed, in a way any Google engineer could have noticed through straightforward testing and, in many instances, in a way Google staff specifically intended. Yet Google lacked authorization for these information collection and distribution practices.

Rogue Google Employees Could Access or Redistribute Book Contents

40. In September 2010, news reports revealed that David Barksdale, a senior Google engineer, had used his privileged position at Google to spy on four teenagers for months.

¹³ J. Nicholas Hoover. "White House Reprimands Deputy CTO." Information Week. May 17, 2010. <http://www.informationweek.com/news/government/leadership/224900083>.

¹⁴ Jonathan Mayer. "Safari Trackers." February 17, 2012. <http://cyberlaw.stanford.edu/blog/2012/02/safari-trackers>.

Because Barksdale was a Site Reliability Engineer at Google, he was able to tap into call logs for Google Voice (records of phone calls to and from the youths), read the youths' instant message chat logs, and unblock himself from buddy lists in order to send instant messages to and from the youths. Barksdale used each of these methods to access the communications of the affected youths. While Google terminated Barksdale's employment after these practices became known, Barksdale was able to continue his practices for months without Google's internal controls noticing what he was doing.¹⁵ Google subsequently admitted that it had previously caught at least one other Google staff person accessing user data without authorization.¹⁶

Hackers Could Access or Redistribute Book Contents

41. Outside hackers could access or redistribute book contents. Many hackers disagree with the public policy embodied in applicable copyright law. For example, during January 2012, hackers disabled web sites of the U.S. Department of Justice and FBI, trade associations Recording Industry Association of America and Motion Picture Association of America, and record labels Universal, BMI, and Warner Music Group, when hackers disapproved of possible revisions to copyright law then under discussion in Congress.¹⁷ Google's digitized book contents thus could attract hackers seeking to redistribute notable information.

42. In January 2010, Google reported a "highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual

¹⁵ Adrian Chen. "GCreep: Google Engineer Stalked Teens, Spied on Chats." Gawker. September 14, 2010. <http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats> .

¹⁶ Jacon Kincaid. "This Is the Second Time a Google Engineer Has Been Fired for Accessing User Data." TechCrunch. September 14, 2010.

¹⁷ Ingrid Lunden. "SOPA Blackout, Anonymous-Style: FBI, DOJ Sites Downed In Megaupload Protest." paidContent.org. January 19, 2012. <http://paidcontent.org/article/419-sopa-blackout-anonymous-style-doj-riaa-hacked-in-megaupload-protest/>.

property from Google.”¹⁸ A subsequent analysis by McAfee indicated that hackers had specifically sought access to the source code for Google systems, and that hackers had even obtained the ability to alter the source code for Google systems.¹⁹ If Google cannot keep its own intellectual property secure from attackers, it is plausible to conclude that Google cannot keep book contents invulnerable to security breaches.

A Single Breach Could Cause Devastating Harm to Authors

43. A single breach of the systems that store book contents could allow book contents to become ubiquitous online. In particular, after that single breach occurs, users are likely to copy and/or share the material en masse, preventing any subsequent efforts to resecure book contents. For example, on August 4, 2006, AOL posted twenty million searches performed by more than 650,000 users over a three-month period. Once AOL realized that posting this information was inadvisable (because it included myriad sensitive subjects and could be easily linked to individual AOL users), AOL removed the file from its servers the same week, but the file remains easily available, including on the web and via BitTorrent.²⁰ Similarly, Wikileaks in February 2010 began publishing hundreds of thousands of pages of classified material. The information remains easily available, including via straightforward Google searches. The information simply cannot be “unpublished” once it has become publicly available on the

¹⁸ David Drummond. Official Google Blog. January 12, 2010. <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html> .

¹⁹ McAfee Labs. “Protecting Your Critical Assets: Lessons Learned from ‘Operation Aurora.’” March 2010. http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf .

²⁰ For example, I searched Google for “AOL search torrent” (without quotes) on March 27, 2012. Among the first ten results, I found six locations where I could download the files. <http://gregsadetsky.com/aol-data/> presents nine different locations where the data remains available.

Internet. The ongoing availability of materials previously distributed via Library.nu – months after Library.nu was shut down by court order – further confirms that once book copies have been freely distributed online, it is virtually impossible to prevent their further redistribution.

44. Thus, if book contents become available once – via a breach of book copies scanned by others, via a breach in libraries’ copies of books scanned by Google, or via a breach of Google’s own systems – the book contents are likely to be available easily and indefinitely.

45. Even if one considers the likelihood to be remote that a particular work will become available through piracy or some other security breach (and I do not think it is remote at all), one must evaluate that risk in light of the devastating effect of such a breach on the rightsholder.

Conclusion

46. It is my opinion that the Defendants’ activities as described above present serious security concerns and put at risk the ability of copyright owners to decide whether and when to exploit electronic copies of their works. This risk will be exacerbated further if Defendants’ practices of digitally copying, and in certain instances, distributing and displaying books without rightsholder permission are found to be fair uses and become widespread. Conversely, requiring Defendants and others to obtain the permission of rightsholders before engaging in such practices could prompt negotiations between rightsholders and those who seek to digitally use their works, thereby fostering standards for the allocation of the costs and risks of any harm flowing from such security breaches.

Dated: Cambridge, MA
June 27, 2012



Benjamin Edelman

EXHIBIT A

Benjamin Edelman – *Curriculum Vitae*

169 Walnut St.
Brookline, MA 02445

Benjamin G. Edelman

ben@benedelman.org
(617) 359-3360

Experience

Assistant professor, Harvard Business School. Negotiations, Organizations & Markets unit. (April 2007 – present)

Fields: Industrial organization, market design, information economics.

Research interests: Electronic markets. Internet advertising, reputation, and fraud. Automated data collection.

Teaching: Networked businesses, market design, information systems, online marketing, negotiation.

Independent consultant and expert witness (November 1999 – present)

Conducted quantitative analyses and empirical testing for a variety of clients including the American Civil Liberties Union, AOL, Microsoft, National Association of Broadcasters, National Football League, New York Times, Universal Music Group, and Washington Post on topics including online advertising, advertising fraud, spyware, spam, pay-per-click advertising and click fraud, Internet filtering, geolocation and targeting, privacy, security, automated data collection, and user interface design.

Qualified as an expert in Federal court on multiple occasions, and provided oral testimony under direct and cross examination.

Student Fellow / Technology Analyst, Berkman Center for Internet & Society (May 1998 – January 2004)

Conducted empirical studies of the Internet's domain name system, spyware/adware, content filtering by network intermediaries.

Developed software systems for interactive real-time communication among class/meeting participants. Designed and operated system for webcast of and remote participation in numerous Berkman Center, Harvard Law School, and Cambridge community events as well as twelve ICANN public meetings.

Education

Harvard Graduate School of Arts & Sciences - Ph.D., Economics, 2007. Dissertation: "Topics in Internet Advertising."

Harvard Law School - J.D., 2005.

Harvard Graduate School of Arts & Sciences - A.M., Statistics, 2002.

Harvard College - A.B., Economics, *summa cum laude*, 2002; Phi Beta Kappa.

Woodrow Wilson Senior High School - Washington, DC: 1998; valedictorian.

Representative Research

Internet Advertising and the Generalized Second Price Auction (*American Economic Review*, 2007)

with Michael Ostrovsky and Michael Schwarz

Optimal Auction Design and Equilibrium Selection in Sponsored Search Auctions (*American Economic Review*, 2010)

with Michael Schwarz

Strategic Bidder Behavior in Sponsored Search Auctions (*Decision Support Systems*, 2007) with Michael Ostrovsky

Measuring the Perpetrators and Funders of Typosquatting (*FC'10, SV LNCS*) with Tyler Moore; web introduction and appendix also available

Greedy Bidding Strategies for Keyword Auctions (*Proceedings of the 9th ACM Conference on Electronic Commerce*, 2007)

with Matthew Cary, Aparna Das, Ioannis Giotis, Kurtis Heimerl, Anna Karlin, Claire Mathieu, and Michael Schwarz

On Best-Response Bidding in GSP Auctions (2008)

with Matthew Cary, Aparna Das, Ioannis Giotis, Kurtis Heimerl, Anna Karlin, Claire Mathieu, and Michael Schwarz

Running Out of Numbers: Scarcity of IPv4 Addresses and What To Do About It (*Proceedings of AMMA*, 2009)

Adverse Selection in Online "Trust" Certifications (*Proceedings of ICEC 2009*)

Adverse Selection in Online "Trust" Certifications and Search Results (*Electronic Commerce Research and Applications*, 2011)

Deterring Online Advertising Fraud Through Optimal Payment in Arrears (*FC'09, SV LNCS*)

Securing Online Advertising: Rustlers and Sheriffs in the New Wild West (published in *Beautiful Security*, 2009)

Assessing and Improving the Safety of Internet Search Engines (published in *The Rising Power of Search Engines on the Internet*, 2006)

Web Sites Sharing IP Addresses: Prevalence and Significance (2003) cyber.law.harvard.edu/people/edelman/ip-sharing

Empirical Analysis of Internet Filtering in China (2002) with Jonathan Zittrain cyber.law.harvard.edu/filtering/china

Published in *IEEE Internet Computing* as "Internet Filtering in China" (March-April 2003)

Long-Term Research Projects

Strategies and Outcomes in Search Engine Advertising (2004-)

“Spyware”: Research, Testing, Legislation, and Suits (2002-) benedelman.org/spyware

Resources for Affiliates and Affiliate Merchants (2004-) benedelman.org/affiliates

Documentation of Internet Filtering Worldwide (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/filtering

The Top-Level Domain Evaluation Project (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/tlds

Classroom and Meeting Technology Tools (1998-2002) cyber.law.harvard.edu/meetingtools

ICANN Public Meeting Archives, Notes, and Briefing Books (1998-2001) cyber.law.harvard.edu/icann cyber.law.harvard.edu/ifwp

Additional Writings

Advertising Disclosures: Measuring Labeling Alternatives in Internet Search Engines (2012)

with Duncan Gilchrist *Information Economics and Policy*

Internet Protocol Numbers and the American Registry for Internet Numbers: Suggested Guidance for Bankruptcy

Trustees, Debtors-in-Possession, and Receivers. *BNA's Bankruptcy Law Reporter* (2012) with Steven Ryan and Matthew Martel

Using Internet Data for Economic Research (2012) *Journal of Economic Perspectives*

Earnings and Ratings at Google Answers (2012) *Economic Inquiry*

Pricing and Efficiency in the Market for IP Addresses (2011) with Michael Schwarz

The Design of Online Advertising Markets (forthcoming) *Handbook of Market Design*

Bias in Search Results?: Diagnosis and Response (2011) *The Indian Journal of Law and Technology*

Measuring Bias in “Organic” Web Search (2011) with Ben Lockwood benedelman.org/searchbias

To Groupon or Not to Groupon: The Profitability of Deep Discounts (2010) *HBS Working Paper* – with Scott Kominers and Sonia Jaffe
and To Groupon or Not To Groupon: New Research on Voucher Profitability (2011) *HBR Blogs*

Least-Cost Avoiders in Online Fraud and Abuse (2010) *IEEE Security and Privacy*

The Pathologies of Online Display Advertising Marketplaces (2010) *ACM Sigecom Exchanges*

Competing Ad Auctions: Multi-homing and Participation Costs (2010) with Itai Ashlagi and Hoan Soo Lee

Priced and Unpriced Online Markets (2009) (*Journal of Economic Perspectives*, summer 2009)

Red Light States: Who Buys Online Adult Entertainment? (2009) (*Journal of Economic Perspectives*, winter 2009)

Who Owns Metrics?: Building a Bill of Rights for Online Advertisers (2009) (*Journal of Advertising Research*, Dec. 2009)

How to Combat Online Ad Fraud (2009) *Harvard Business Review*

The Dark Underbelly of Online Advertising (2009) *Harvard Business Review Online – HBR Now*

Fraud in Online Advertising (2009) *The Business Standard (India)*

Typosquatting: Unintended Adventures in Browsing (2008) *McAfee Security Journal*

CPC/CPA Hybrid Bidding in a Second Price Auction (2008) with Hoan Soo Lee

When the Net Goes Dark and Silent (2002) *South China Morning Post* (op-ed)

The Effect of Editorial Discretion Book Promotion on Sales at Amazon.com (2001-2002) benedelman.org/pubs/thesis-intro.pdf
Seymour and Ruth Harris Prize for Best Thesis in Economics, Thomas Temple Hoopes Prize for Undergraduate Research

Web Site Writings

Flash-Based Cookie-Stuffer Using Google AdSense to Claim Unearned Affiliate Commissions from Amazon (2012)
benedelman.org/news/050712-1.html with Wesley Brandi

Search My Logs of Affiliate Fraud and Affiliate Fraud Information Lookup (2012) with Wesley Brandi

Hack-Based Cookie-Stuffing by Bannertracker-script (2012) benedelman.org/news/022712-1.html with Wesley Brandi

Large-Scale Cookie-Stuffing at Eshop600.co.uk (2012) benedelman.org/news/013012-1.html with Wesley Brandi

Advertising Disclosures in Online Apartment Search (2012) benedelman.org/adlabeling/apartmentsearch with Paul Kominers

Google Tying Google Plus and Many More (2012) benedelman.org/news/011212-1.html

Revisiting Search Bias at Google (2011) benedelman.org/news/111111-1.html

Understanding the Purposes – and Weaknesses – of Online-to-Offline Discounting Pymnts.com (2011)

Towards Improvement in Singapore’s Transportation Efficiency and Environmental Impact (2011)
submission to the National Climate Change Secretariat of Singapore

Google’s Dominance – And What To Do About It and Finding and Preventing Biased Results (2011)
American Constitution Society for Law and Policy – Blog Debate

Advertisers’ Missing Perspective in the Google Antitrust Hearing (2011) benedelman.org/news/092011-1.html

Implications of Google’s Pharmacy Debacle (2011) benedelman.org/news/082611-1.html and republished at Betanews

Online Discount Vouchers – Letter-Writing Tool (2011) vouchercomplaints.org with Paul Kominers and Xiaoxiao Wu

Consumer Protection in Online Discount Voucher Sales (2011) benedelman.org/voucher-consumer-protection with Paul Kominers

Revisiting Unlawful Advertisements at Google (2011) benedelman.org/news/051811-1.html and excerpted at Huffington Post

Personal Rapid Transport - Environmental Issues for Earth Day (2011) hbs.edu/news/releases/earthday042011.html

Remedies for Search Bias (2011) benedelman.org/news/022211-1.html

In Accusing Microsoft, Google Doth Protest Too Much (2011) *HBR Blogs*

Knowing Certain Trademark Ads Were Confusing, Google Sold Them Anyway -- for \$100+ Million (2010)
benedelman.org/news/113010-1.html

Advertisers Should Raise Their Voices Against Arrogant Google (2010) *mUmBRELLA*

Hard-Coding Bias in Google ‘Algorithmic’ Search Results (2010) benedelman.org/hardcoding

A Closer Look at Google's Advertisement Labels (2010) benedelman.org/adlabeling/google-nov2010.html

On Facebook and Privacy (2010) www.hbs.edu/news/releases/facultyonfacebookprivacy.html

Tying Google Affiliate Network (2010) benedelman.org/news/092810-1.html

Facebook Leaks Usernames, User IDs, and Personal Details to Advertisers (2010) benedelman.org/news/052010-1.html

Sony’s Crackle: Invisible Traffic Galore (2010) benedelman.org/news/042710-1.html

Protecting Privacy by Design (2010) *McAfee AVERT Blog*

Google’s Privacy Breach: Lessons for Companies (2010) *Harvard Business Review Online – HBR Now*

Google Toolbar Tracks Browsing Even After Users Choose “Disable” (2010) benedelman.org/news/012610-1.html

Upromise Savings -- At What Cost? (2010) benedelman.org/news/012110-1.html

Google Still Charging Advertisers for Conversion-Inflation Traffic (2010) benedelman.org/news/010510-1.html

Towards a Bill of Rights for Online Advertisers (2009) benedelman.org/advertisersrights
(excerpted in Advertising Week Welcome Guide, excerpted in Huffington Post)

Payment Card Network Rules Prohibit Aggressive Post-Transaction Tactics (2009) benedelman.org/posttransaction/cardnetworks

Deception in Post-Transaction Marketing Offers (2009) benedelman.org/posttransaction (including Senate testimony)

How Google and Its Partners Inflate Measured Conversion Rates and Increase Advertisers’ Costs (2009)
benedelman.org/news/051309-1.html

In Support of Utah’s HB450 (2009) benedelman.org/news/030909-1.html

False and Deceptive Display Ads at Yahoo’s Right Media (2009) benedelman.org/rightmedia-deception

Privacy Lapse at Google JotSpot (2008) benedelman.org/google-jot-privacy

Hydra Media's Pop-Up Problem -- Ten Examples (2008) benedelman.org/news/101408-1.html

CPA Advertising Fraud: Forced Clicks and Invisible Windows (2008) benedelman.org/news/100708-1.html

Auditing Spyware Advertising Fraud: Wasted Spending at VistaPrint (2008) benedelman.org/news/093008-1.html

PPC Platform Competition and Google's "May Not Copy" Restriction (2008) benedelman.org/news/062708-1.html

Debunking Zango's "Content Economy" (2008) benedelman.org/news/052808-1.html

Coupons.com and TRUSTe: Lots of Talk, Too Little Action (2008) benedelman.org/news/031808-1.html

Delaying Payment to Deter Online Advertising Fraud (2008) benedelman.org/paymentdelay

Critiquing C-NetMedia's Anti-Spyware Offerings and Advertising Practices (2008) benedelman.org/news/021408-1.html

Sears Exposes Customer Purchase History in Violation of Its Privacy Policy (2008) benedelman.org/news/010408-1.html

The Sears "Community" Installation of ComScore (2008) benedelman.org/news/010108-1.html

A Closer Look at Coupons.com (2007) benedelman.org/news/082807-1.html

Spyware Still Cheating Merchants and Legitimate Affiliates (2007) benedelman.org/news/052107-1.html

How Spyware-Driven Forced Visits Inflate Web Site Traffic Counts (2007) benedelman.org/news/050707-1.html

Advertising Through Spyware -- After Promising To Stop (2007) benedelman.org/news/031407-1.html

Why I Can Never Agree with Adware and Spyware (2007) technology.guardian.co.uk/online/insideit/story/0,,1997629,00.html

Bad Practices Continue at Zango (2006) with Eric Howes benedelman.org/news/112006-1.html

Intermix Revisited (2006) benedelman.org/news/110806-1.html

Current Ask Toolbar Practices (2006) benedelman.org/spyware/ask-toolbars

False and Deceptive Pay-Per-Click Ads (2006) benedelman.org/ppc-scams

Cookies Detected by Anti-Spyware Programs: The Current Status (2006) www.vinnylingham.com/specialreports/cookie-detections

How Vonage Funds Spyware (2006) benedelman.org/news/071806-1.html

Spyware Showing Unrequested Sexually-Explicit Images (2006) benedelman.org/news/062206-1.html

Banner Farms in the Crosshairs (2006) benedelman.org/news/061206-1.html

The Safety of Internet Search Engines (2006) siteadvisor.com/studies/search_safety_may2006 with Hannah Rosenbaum

New York v. Direct Revenue, LLC - Documents and Analysis (2006) benedelman.org/spyware/nyag-dr

The Spyware - Click-Fraud Connection - and Yahoo's Role Revisited (2006) benedelman.org/news/040406-1.html

Advertisers Funding Direct Revenue (2006) benedelman.org/spyware/images/dr-mar06

Critiquing ITSA's Pro-Adware Policy (2006) benedelman.org/news/033106-2.html

Advertisers Funding 180solutions (2006) benedelman.org/spyware/images/180-jan06

Nonconsensual 180 Installations Continue (2006) benedelman.org/news/022006-1.html

Pushing Spyware through Search (2006) benedelman.org/news/012606-1.html

Affiliate Hall of Shame (2006) benedelman.org/news/011606-1.html

180solutions's Misleading Installation Methods - Dollidol.com (2006) benedelman.org/spyware/installations/dollidol-180

Scanning for Solutions (2005) publications.mediapost.com/index.cfm?fuseaction=Articles.san&s=37284

What Claria Doesn't Disclose (Any More) (2005) benedelman.org/news/111505-1.html

Claria Shows Ads Through Exploit-Delivered Popups (2005) benedelman.org/news/101805-1.html

Video: New.net Installed through Security Holes (2005) benedelman.org/news/100505-1.html

How Affiliate Programs Fund Spyware (2005) benedelman.org/news/091405-1.html

How Expedia Funds Spyware (2005) benedelman.org/news/090705-1.html

How Yahoo Funds Spyware (2005) benedelman.org/news/083105-1.html

What Passes for “Consent” at 180solutions (2005) benedelman.org/news/062805-1.html

Google’s Role: Syndicated Ads Shown Through Ill-Gotten Third-Party Toolbars (2005) benedelman.org/news/060605-1.html

Ask Jeeves Toolbar Installs via Banner Ads at Kids Sites (2005) benedelman.org/spyware/installations/askjeeves-banner

Hotbar Installs via Banner Ads at Kids Sites (2005) benedelman.org/spyware/installations/kidzpage-hotbar

The 180 Turnaround That Wasn’t (2005) adbumb.com/adbumb159.html

The PacerD Installation Bundle (2005) benedelman.org/spyware/installations/pacerd

Claria’s Misleading Installation Methods - Ezone.com (2005) benedelman.org/spyware/installations/ezone-claria

Claria’s Misleading Installation Methods - Dope Wars (2005) benedelman.org/spyware/installations/dopewars-claria

180solutions’s Misleading Installation Methods - Ezone.com (2005) benedelman.org/spyware/installations/ezone-180

3D Desktop’s Misleading Installation Methods (2005) benedelman.org/spyware/installations/3d-screensaver

Comparison of Unwanted Software Installed by P2P Programs (2005) benedelman.org/spyware/p2p

Advertisers Supporting eXact Advertising (2005) benedelman.org/spyware/exact-advertisers

How Google’s Blogspot Helps Spread Unwanted Software (2005) benedelman.org/news/022205-1.html

How VeriSign Could Stop Drive-By Downloads (2005) benedelman.org/news/020305-1.html

Intermediaries’ Role in the Spyware Mess (2005) benedelman.org/news/052305-1.html

Media Files that Spread Spyware (2005) benedelman.org/news/010205-1.html

Video: Ebates Installed through Security Holes (2004) benedelman.org/news/121504-1.html

Direct Revenue Deletes Competitors from Users’ Disks (2004) benedelman.org/news/120704-1.html

Who Profits from Security Holes? (2004) benedelman.org/news/111804-1.html

Gator’s EULA Gone Bad (2004) benedelman.org/news/112904-1.html

Grokster and Claria Take Licenses to New Lows, and Congress Lets Them Do It (2004) benedelman.org/news/100904-1.html

California’s Toothless Spyware Law (2004) benedelman.org/news/092904-1.html

The Effect of 180solutions on Affiliate Commissions and Merchants (2004) benedelman.org/spyware/180-affiliates

WhenU Spams Google, Breaks Google “No Cloaking” Rules (2004) benedelman.org/spyware/whenu-spam

WhenU Copies 26+ Articles from 20+ News Sites (2004) benedelman.org/spyware/whenu-copy

Advertisers Using WhenU (2004) benedelman.org/spyware/whenu-advertisers

WhenU Security Hole Allows Execution of Arbitrary Software (2004) benedelman.org/spyware/whenu-security

WhenU Violates Own Privacy Policy (2004) benedelman.org/spyware/whenu-privacy

Methods and Effects of Spyware (FTC Comments) (2004) benedelman.org/spyware/ftc-031904.pdf

A Close Reading of Utah’s Spyware Control Act (2004) benedelman.org/spyware/utah-mar04

Blocked Sites will Return, but with Limited Access (2003) South China Morning Post (op-ed)

Web Sites Sharing IP Addresses: Prevalence and Significance (2003) cyber.law.harvard.edu/people/edelman/ip-sharing

Documentation of Gator Advertisements and Targeting (2003) cyber.law.harvard.edu/people/edelman/ads/gator

Empirical Analysis of Google SafeSearch (2003) cyber.law.harvard.edu/people/edelman/google-safesearch

Large-Scale Registration of Domains with Typographical Errors (2003) cyber.law.harvard.edu/people/edelman/typo-domains

Technical Responses to Unilateral Internet Authority: The Deployment of VeriSign “Site Finder” and ISP Response (2003) with Jonathan Zittrain cyber.law.harvard.edu/tlds/sitefinder

Compliance with UDRP Decisions: A Case Study of Joker.com (2003) cyber.law.harvard.edu/people/edelman/udrp-compliance

Domain Name Typosquatter Still Generating Millions (2003) circleid.com/article/101_0_1_0_C

Localized Google Search Result Exclusions (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/filtering/google

Defensive Registrations: Why They’re Still Needed, and How to Make Them Earn Their Keep (2002)
Verisign Digital Brand Management Digital Branding Bulletin, www.verisign.com/services/cdns/news/columnist_200212.html

Documentation of Internet Filtering in Saudi Arabia (2002) with Jonathan Zittrain cyber.law.harvard.edu/filtering/saudi-arabia

Localized Google Search Result Exclusions (2002) with Jonathan Zittrain cyber.law.harvard.edu/filtering/filtering/google

Analysis of Domain Reregistrations Used for Distribution of Sexually-Explicit Content (2002)
cyber.law.harvard.edu/people/edelman/renewals

Large-Scale Intentional Invalid WHOIS Data (2002) cyber.law.harvard.edu/people/edelman/invalid-whois

.NAME Registrations Not Conforming to .NAME Registration Restrictions (2002)
cyber.law.harvard.edu/people/edelman/name-restrictions

Alternative Perspectives on Registrar Market Share (2002) cyber.law.harvard.edu/people/edelman/registrar-choice

DNS as a Search Engine: A Quantitative Evaluation (2002) cyber.law.harvard.edu/people/edelman/dns-as-search

Disputed Registrations in .BIZ (2002) cyber.law.harvard.edu/people/edelman/biz-sunrise

TLD Registration Enforcement: A Call for Automation (2002) circleid.com/article/66_0_1_0_C circleid.com/article/72_0_1_0_C

Invalid WHOIS Data: Who Is Responsible? (2002) circleid.com/article/79_0_1_0_C

iCraveTV.biz/Entertainment Tonight Retransmits CNN, Cartoon Network, PAX TV, California NBC Affiliate (2002)
cyber.law.harvard.edu/people/edelman/icrave

Analysis of Registrations in Alternative Root TLDs (2001) cyber.law.harvard.edu/people/edelman/dotbiz and [/people/edelman/dotweb](http://people/edelman/dotweb)

Documentation of Privacy and Security Shortcomings at Buy.com (2000) cyber.law.harvard.edu/people/edelman/buy-privacy.html

Understanding and Critiquing ICANN’s Policy Agenda (2000) cyber.law.harvard.edu/icann/pressingissues2000/briefingbook

Software Environments for Online Deliberative Discourse (1999-2000) cyber.law.harvard.edu/projects/deliberation

Executive Summaries of Formative ICANN Documents (1999)
cyber.law.harvard.edu/pressbriefings/icann/briefingbook/executivesummaries.html

ICANN and the Public Interest: Pressing Issues (1999) cyber.law.harvard.edu/icann/workshops/la/briefingbook

Using Trumpet Winsock on Netcom Netcruiser Accounts (1995) cyber.law.harvard.edu/people/edelman/trumpet.html

Teaching Cases and Notes

Airbnb (A) and (B) (HBS Case 912-019, -020) (and TN) (2011) with Michael Luca

Attack of the Clones: Birchbox Defends Against Copycat Competitors (HBS Case 912-010) (2011) with Peter Coles

The Online Economy: Strategy and Entrepreneurship - Course Architecture Note (HBS Note 911-069) (2011) with Peter Coles

Mobilizing Online Businesses (HBS Module Note 911-048) (2011) with Peter Coles

Online Marketing at Big Skinny (HBS Case 911-033) (and TN) (2011) with Scott Kominers

The iPhone at IVK (TN) (HBS Teaching Note 911-414) (2010)

Akamai, Inc. (HBS Case 804-158) (2010) with Thomas Eisenmann and Eric Van den Steen

Google Inc. and Google Inc. (Abridged) (HBS Case 910-036 and 910-032) (2010) (and TN) with Thomas Eisenmann

Personal Rapid Transport at Vectus, Inc. (HBS Case 910-010) (2010) (and TN)

eBay Partner Network (A), (B), and (C) (HBS Case 910-008, -009, and -012) (2009) (and TN) with Ian Larkin

Symbian, Google & Apple in the Mobile Space (A) and (B) (HBS Case 909-055, -056) (2009) with F. Suarez & A. Srinivasan
 Distribution at American Airlines (A) and (B) (HBS Case 909-035 and -036) (and TN) (2009)
 Windows Vista (HBS Case 909-038) (2009)
 Online Restaurant Promotions (HBS Case 909-034) (and TN) (2009)
 Ad Classification at Right Media (HBS Case 909-032) (and TN) (2009)
 Consumer Payment Systems – United States (HBS Case 909-006) (2009) (and TN) with Andrei Hagiu
 Consumer Payment Systems – Japan (HBS Case 909-007) (2009) (and TN) with Andrei Hagiu
 TheLadders (HBS Case 908-061) (2008) (and TN) with Peter Coles, Brian Hall, and Nicole Bennett
 Opening Dot EU (A) and (B) (HBS Case 908-052 and -053) (2008)
 Microsoft adCenter (HBS Case 908-049) (and TN) (2008) with Peter Coles

Programming Experience

Microsoft Visual Basic (15+ years experience), VB.NET	Mathworks MatLab	Stata
SPlus / R	Python	PHP

Awards

Emerald Citations of Excellence Award (2011)
 ECCH Award for Outstanding Contribution to the Case Method – Strategy and General Management (2011)
 Best Paper Award, Honorable Mention – The 11th International Conference on Electronic Commerce (2009)
 Harvard University Graduate Economics Fellowship (2003-2006)
 John M. Olin Fellowship in Law and Economics (2003-2004, 2004-2005)
 Hoopes Prize for Undergraduate Research (2002)
 Seymour and Ruth Harris Prize for Best Honors Thesis in Economics (2002)
 John Harvard Scholarship, Harvard College (1998-1999, 1999-2000, 2000-2001)
 Rank I Honors, Harvard College (1998-1999, 1999-2000, 2000-2001)
 Phi Beta Kappa, Harvard College (2001)
 Undergraduate Honors Research Scholarship, Department of Economics, Harvard College (2001)
 Detur Prize, Harvard College (1999)

Congressional and Expert Testimony

US Senate, Commerce Committee (2009) (statement for the record)
 US House of Representatives, Committee on the Judiciary (2008) (invited / hearing cancelled)
 US Senate, Committee on Commerce, Science, and Transportation (2008)
 Federal Trade Commission Public Hearing on Effectiveness of CAN-SPAM (2005)
 District Court, Third Judicial District of Utah (2004)
 US Federal Court, Eastern District of Michigan (2003)
 US House of Representatives, Committee on the Judiciary (2003)
 US Federal Court, Eastern District of Pennsylvania (2002)
 US Federal Court, Western District of Pennsylvania (2000)

Academic Service

Associate Editor: Journal of Economic Perspectives (2008-2012)

Referee: American Economic Review, Quarterly Journal of Economics, Journal of Applied Economics, RAND Journal of Economics, Management Science, Journal of Economics & Management Strategy, Sponsored Search Workshop, Workshop on the Economics of Information Security, Workshop on the Economics of Securing the Information Infrastructure, Manufacturing & Services Operations Management, The International Conference on Electronic Commerce (2009), International Review of Law and Economics, Journal of Industrial Economics, Operations Research, Berkeley Electronic Press – Policy & Internet, Review of Economic Studies, Economics Letters, Management Science, Review of Industrial Organization, Telecommunications Policy, Emerald Program, National Science Foundation, Manufacturing and Service Operations Management

Program committee: Workshop on the Economics of Securing the Information Infrastructure (2006), Sponsored Search Workshop (2007), WWW2008, Fourth Workshop on Ad Auctions (2008), The First Conference on Auctions, Market Mechanisms and Their Applications (2009), ACM Conference on Electronic Commerce (2010), Workshop on the Economics of Information Security (2010), Workshop on the Economics of Information Security (2011), Seventh Workshop on Ad Auctions (2011), The Second Conference on Auctions, Market Mechanisms and Their Applications (2011), WWW2012, Anti-Phishing eCrime Researchers Summit (2012)

Co-organizer: Sixth Workshop on Ad Auctions (2010)

Non-resident tutor / senior common room member: Cabot House (2004-2012)


EXHIBIT B**Benjamin Edelman – Prior Testimony at Trial or Deposition**

Proceeding	Court	Reference	Context	Year	On behalf of
National Football League, et al. v. TVRADIONOW Corporation, et al.	U.S. District Court, Western District of Pennsylvania	No. Civ.A. 00-120 and 00-121	Hearing	2000	Plaintiff
Multnomah County Public Library, et al. v. United States of America	U.S. District Court, Eastern District of Pennsylvania	No. Civ.A. 01-1322	Deposition, hearing	2002	Plaintiff
Washingtonpost.Newsweek Interactive Company, LLC, et al. v. The Gator Corporation	U.S. District Court, Eastern District of Virginia	02-909-A	Deposition	2002	Plaintiff
Wells Fargo & Company, et al., v. WhenU.com, Inc.	U.S. District Court, Eastern District of Michigan	03-71906	Deposition, hearing	2003	Plaintiff
WhenU.com, Inc. v. The State of Utah	Utah District Court	Civ. No. 040907478	Hearing	2004	Defendant
The People of the State of California ex. rel. Rockard J. Delgadillo, Los Angeles City Attorney v. Intermix Media, Inc.	Los Angeles Superior Court	BC343196	Deposition	2006	Plaintiff
State of South Carolina v. Casale Media, Inc., et al.	South Carolina Court of Common Pleas, Richland County	08-CP-40-0729	Deposition	2008	Plaintiff
UMG Recordings, Inc., et al. v. Veoh Networks, Inc., et al.	U.S. District Court, Central District of California	No. CV 07-5744 AHM (AJWx)	Deposition	2009	Plaintiff
Netscape Communications Corp. v. Valueclick, Inc., et al.,	U.S. District Court, Eastern District of Virginia	No. 1:09-cv-225-TSE-IDD	Deposition	2009	Plaintiff
Arista Records, et al., v. Myxer, Inc., et al.	U.S. District Court, Central District of California	No. CV 08-03935 GAF (JCx)	Deposition	2009	Plaintiff
Stephanie Lens v. Universal Music Corp., et al.	United States District Court, Northern District of California	No. C 07-03783 JF (PVT)	Deposition	2010	Defendant
Authors Guild v. Google Inc.	United States District Court, Southern District of New York	No. 05 Civ. 8136 (DC)	Deposition	2012	Plaintiff

EXHIBIT C

Benjamin Edelman – Materials Considered

In addition to the materials cited in my declaration, I have considered the following documents:

1. First Amended Complaint in *The Authors Guild Inc., et al., v. Hathitrust, et al.*;
2. Plaintiffs' Brief in Support of Motion for Partial Judgment on the Pleadings in the Authors Guild v. Hathitrust case;
3. Plaintiffs' Fourth Amended Class Action Complaint in *The Authors Guild Inc., et al. v. Google Inc.*;
4. Google's Objections and Responses to Plaintiffs' First Set of Requests for Admission in *The Authors Guild Inc., et al. v. Google Inc.*;
5. Plaintiffs' Class Certification Brief in *The Authors Guild Inc., et al. v. Google Inc.*;
6. Transcript from the declaration of Joanne Zack and exhibits in support of Plaintiffs' Class Certification Motion in *The Authors Guild Inc., et al. v. Google Inc.*;
7. Google's Brief in Opposition to Plaintiffs' Motion for Class Certification in *The Authors Guild Inc., et al. v. Google Inc.*;
8. Plaintiffs' Brief in Opposition to Defendant's Motion to Dismiss the Authors Guild as Associational Plaintiff in *The Authors Guild Inc., et al. v. Google Inc.*;
9. Declarations of Daniel Clancy, dated February 11, 2010, and February 7, 2012 in *The Authors Guild Inc., et al. v. Google Inc.*;
10. Google's Supplemental Responses and Objections to Plaintiffs' Second Request for Production of Documents and Things (Public Redacted Version);
11. Cooperative Agreement between Google and the University of Michigan;
12. Cooperative Agreement between Google and the University of California;
13. Transcript from the deposition of John Wilkin (HathiTrust/University of Michigan) dated April 25, 2012;
14. Transcript from the deposition of Dan Clancy (Google) dated June 1, 2012;
15. 
16. Google Books website at <http://books.google.com>.