

BookGlutton Content Protection

A recommendation for evaluating new services

Aaron Miller

Travis Alber

BookGlutton.com

BookGlutton is a new type of service for book consumers. Instead of providing downloads of purchased books, BookGlutton makes books accessible from any device with a web browser. By providing a rich, social reading experience that rivals any desktop or device reading experience, BookGlutton hopes to change the way books are purchased, delivered and read.

Unlike many desktop applications and hardware devices, an entirely web-based service means book files are never "in the wild." Instead of files being burned to media or uploaded to The Pirate Bay, all sharing and recommendation takes place through the delivery service itself.

Until recently, people hadn't thought too much about the prospect of consuming a commercial book in a web browsing environment. But a new equation has emerged for publishers who are looking at the profit potential of this new medium. Advances in web-based layout and typography alongside technology like AJAX have enabled new levels of responsiveness and elegance in web applications. A browser-based reading experience can also be superior to any other digital reading experience simply because of its potential for integration with the rest of the web (think community, social channels, metadata, and video and audio supplements). New business models that respect this possibility will lower costs for consumers and raise profits for publishers and authors, while still protecting the rights associated with book content.

This issue of content protection is vital to our business. Internally, we protect content the way we protect credit card information: with firewalls, dedicated hardware, a secure and managed facility, 24-7 monitoring and reporting, and encrypted connections and feeds for customer and publisher data. Since the actual consumption of the content also takes place in this system, we can constantly monitor abuse or illegal copying. This means that, unlike providers of desktop apps or hardware, we can respond instantly with security patches.

The nature of sharing on our service is linking, not copying. On the web, consumers would much rather have links than files. They would also much rather share a clipping or snippet of text than an entire book. That said, the illegal copying and redistribution of text is still a concern for publishers and authors. Once the text of a book is displayed in a browser, it's susceptible to copying. Steps taken to address this concern usually involve some combination of the following measures:

- 1.) Dynamically generating the HTML to display pages, so "viewing source" doesn't reveal it.
- 2.) Chunking files into smaller segments to prevent outright copying of an entire file

- 3.) Chunking text to prevent outright copying of long passages
- 4.) Disabling right-click mouse actions or key presses such as CTRL-C
- 5.) Disabling the ability to select text
- 6.) Using Flash or some other plugin to protect text when it's displayed in the browser
- 7.) Creating images of each page

BookGlutton employs some of these. To employ all of them would seriously undermine the quality of the reading experience. Briefly, here is how we address each:

Disabling view source and Dynamic content generation

On BookGlutton, a user cannot lift text by viewing the page source, because we use dynamic content generation. In simple terms, the text of each page is not part of the HTML document, so the normal browser means of viewing that source code will not reveal it.

Chunking of files

Although we use the EPUB format, those files are never transferred to the browser. Instead, our system outputs only the portions of the EPUB file which the user has access to, and it does so one section at a time. Our system allows for selective control of which sections in an EPUB get sent to the browser.

Chunking of text content

Put simply, this refers to pagination. Text from a book is only displayed in page-sized chunks, one page at a time. Since a digital "page" is a variable run defined by screen and font size, often the amount of text per page is less than what fits on a printed page, so, for example, a 300-page book on paper might become a 1,000 page book on the screen. On a mobile device, it might be 5,000 pages.

Disabling right click

We don't disable right-clicking, because we think right-clicking is useful. We may someday repurpose it to display an action menu different from the typical browser menu. Actions in such a menu would not include copy and paste but would present options like share, annotate, highlight, mark for discussion, etc.

Disabling selection of text

We don't disable the selection of text because ultimately we want people to be able to annotate selected portions of text, or link to granular chunks of each page. This is how people expect to use the Web, and allowing it generates more overall interest in content. It gets harder to discuss a book when you can't select something to spark discussion.

Using Flash, plugins or extensions

We've built our platform on open, vendor-neutral standards with very wide adoption. We want to guarantee the widest reach as a distribution platform, and don't want to be dependent on non-neutral standards or technologies that are not supported on some mobile devices.

Creating images of each page

We are also committed to the emerging EPUB standard and reflowable books, so creating images of the pages severely limits the screen sizes on which our books can be read, makes text less legible, and goes against the intentions and purpose of the EPUB format.

To summarize, while encrypting files protects them "in the wild," it does very little when they are already in a highly secure web system. Using Adobe's form of EPUB encryption, for example, in a web system would require decrypting book content before sending it to the browser, which would defeat the purpose of the encryption. Besides, the web already offers strong encryption for securing that content in its path from server to browser, and it's the same encryption used to transmit passwords and credit card numbers: SSL.

New criteria are needed for evaluating the risks of web-based services. Instead of vetting a service based on whether it licenses and uses a particular form of file encryption or DRM, it's far better to require the following:

- 1.) Users identify themselves before purchasing, sharing or consuming content
- 2.) Content is chunked, and the entire file is never available to the consumer
- 3.) The platform is based on linking, not copying
- 4.) The service and the content are tied together, so that one without the other represents a significant drop in value for the consumer
- 5.) The service's network architecture meets the same stringent requirements for the storing of credit card data and other sensitive information, meaning:
 - a.) It runs on dedicated hardware in a secure facility
 - b.) It transfers files and sensitive data from publishers over secure, encrypted channels
 - c.) It has 24-7 monitoring, reporting and alerting, so compromises and abuse are instantly addressable

We are headed quickly into a future where almost all intellectual commodities get distributed through the web. Instead of fearing this, we need to face the reality that the web is the one network that empowers people to find exactly what they're looking for, and enjoy it with others. That's something people are willing to pay for. The "long tail" of publishing will be on the Web, as it has been for other industries, and we hope you look forward to it as much as we do.