Michael A. Rolenz
12 December, 2002
"Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies"

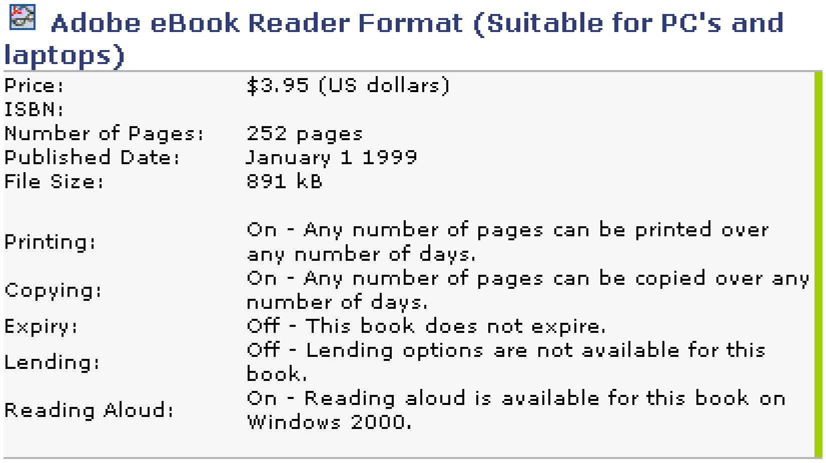
1. Descriptive Name Class : Works in the Public Domain that have been distributed using access controls.

Summary:

Works in the Public Domain may not be copyrighted. Circumvention of access controls for Public Domain works can not be a violation of 17 U.S.C. 1201(a)(1)(C) since that section refers only to copyrighted works.

Facts and evidence:

Adobe Corporation has an electronic format called ebooks. From their website there are numerous works in the public domain. One such is Robert Lewis Stevenson's "Treasure Island"[1]. One such work is available for $3.95 with the following restrictions. (http://www.ebooks.com/items/item-display.asp?IID=11079)

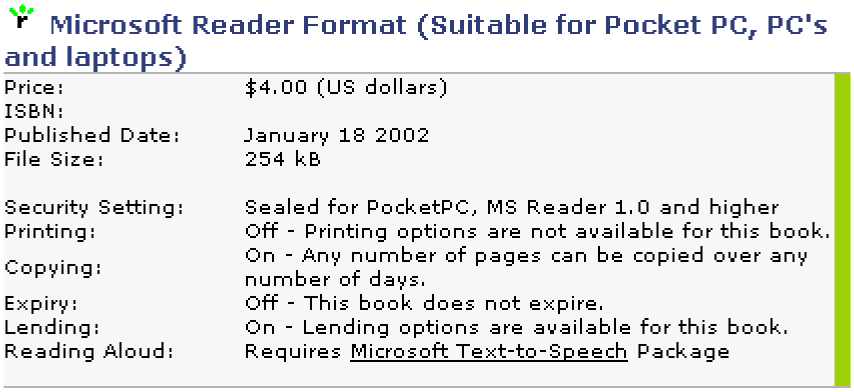


Adobe eBook Reader Format (Suitable for PC's and laptops)

Price:	$3.95 (US dollars)
ISBN:	
Number of Pages:	252 pages
Published Date:	January 1 1999
File Size:	891 kB
Printing:	On - Any number of pages can be printed over any number of days.
Copying:	On - Any number of pages can be copied over any number of days.
Expiry:	Off - This book does not expire.
Lending:	Off - Lending options are not available for this book.
Reading Aloud:	On - Reading aloud is available for this book on Windows 2000.

Another is available for $4.00 with these restrictions.(http://www.ebooks.com/items/item-display.asp?IID=27286)

[1] Which I might add is the basis for a recent Disney film called "Treasure Planet."

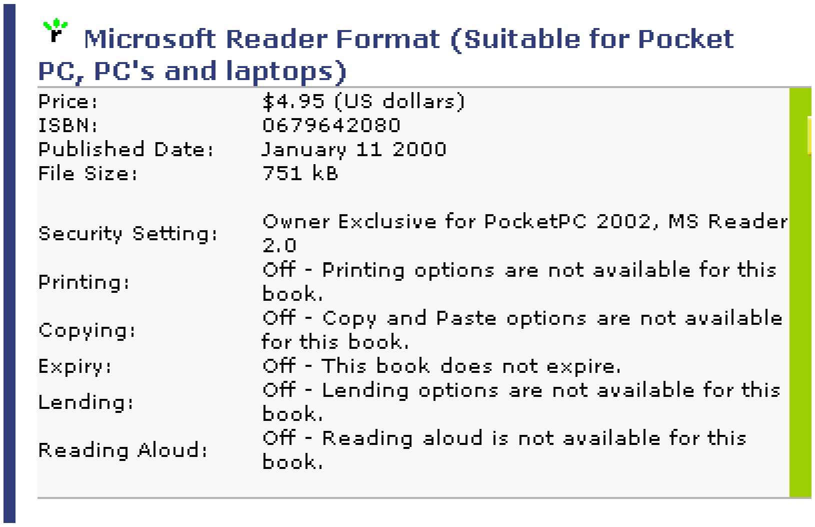


Microsoft Reader Format (Suitable for Pocket PC, PC's and laptops)

Price:	$4.00 (US dollars)
ISBN:	
Published Date:	January 18 2002
File Size:	254 kB
Security Setting:	Sealed for PocketPC, MS Reader 1.0 and higher
Printing:	Off - Printing options are not available for this book.
Copying:	On - Any number of pages can be copied over any number of days.
Expiry:	Off - This book does not expire.
Lending:	On - Lending options are available for this book.
Reading Aloud:	Requires Microsoft Text-to-Speech Package

Notice that one can print one version and not the other; yet the work is in the public domain.

Or in the case of Walt Whitman (http://www.ebooks.com/items/item-display.asp?IID=24830)

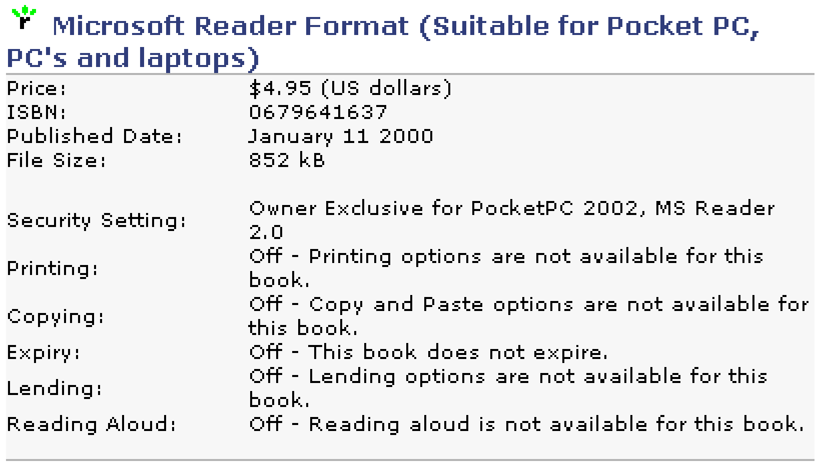


Microsoft Reader Format (Suitable for Pocket PC, PC's and laptops)

Price:	$4.95 (US dollars)
ISBN:	0679642080
Published Date:	January 11 2000
File Size:	751 kB
Security Setting:	Owner Exclusive for PocketPC 2002, MS Reader 2.0
Printing:	Off - Printing options are not available for this book.
Copying:	Off - Copy and Paste options are not available for this book.
Expiry:	Off - This book does not expire.
Lending:	Off - Lending options are not available for this book.
Reading Aloud:	Off - Reading aloud is not available for this book.

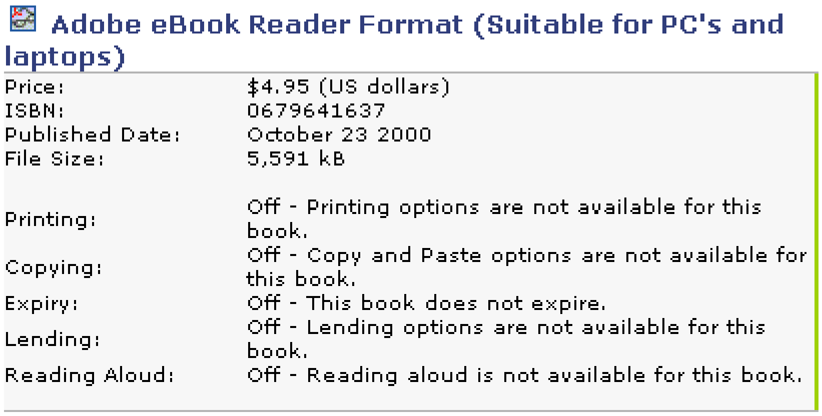
One cannot print out a copy of his works.

Next consider John Keats (http://www.ebooks.com/items/item-display.asp?IID=15675)



Microsoft Reader Format (Suitable for Pocket PC, PC's and laptops)

Price:	$4.95 (US dollars)
ISBN:	0679641637
Published Date:	January 11 2000
File Size:	852 kB
Security Setting:	Owner Exclusive for PocketPC 2002, MS Reader 2.0
Printing:	Off - Printing options are not available for this book.
Copying:	Off - Copy and Paste options are not available for this book.
Expiry:	Off - This book does not expire.
Lending:	Off - Lending options are not available for this book.
Reading Aloud:	Off - Reading aloud is not available for this book.



Adobe eBook Reader Format (Suitable for PC's and laptops)

Price:	$4.95 (US dollars)
ISBN:	0679641637
Published Date:	October 23 2000
File Size:	5,591 kB
Printing:	Off - Printing options are not available for this book.
Copying:	Off - Copy and Paste options are not available for this book.
Expiry:	Off - This book does not expire.
Lending:	Off - Lending options are not available for this book.
Reading Aloud:	Off - Reading aloud is not available for this book.

Not only can one not print, lend, or read aloud the work but one cannot even copy a quotation electronically.

What have we here then? To access public domain works one requires particular software of a particular version (which may or may not be available or compatible with future versions). One is prevented from printing out paper copies which one was previously free to do with public domain works. One cannot even LEND a public domain work to someone electronically even if one could print out a paper copy and send it to them. One is prevented from using those works to create derivative works (e.g., speech synthesizers) and in the last instance quotation is fair use even had the material been COPYRIGHTED. Furthermore, these ebooks are even more expensive than many of the hardback or paper back editions that are available! Doubtless more egregious examples can be found but these were the first four ebooks I selected on the Adobe ebooks website that I knew to be in the public domain since all authors died in the 19th century. What should be considered also is that whether or not Adobe or others change the accesses of later distributions of public domain works, under the DMCA, the accesses of earlier ones still have the force of law.

Argument:

As the Librarian of Congress has stated “ The statutory focus of this rulemaking is limited to one subsection of section 1201: The prohibition on the conduct of circumvention of technological measures that control access to copyrighted works“ which restates the Digital Millennium Copyright Act (DMCA). Works in the Public Domain are not copyrighted and so do not fall within the scope of the DMCA. Furthermore, the act of converting Public Domain works to digital formats does not render those works eligible for copyright protection because the work is not original. It is well established jurisprudence that typesetting of facts or of public domain works do not impart enough originality to a those works to satisfy the requirement for copyright. If not the laborious manual setting of individual letters of cast lead in from the typebox of a printer, then surely the scanning, optical character recognition, spell checking of computers followed by proofreading of the result does not either. Neither does copying the computer file that someone has already generated and placed on the Internet and then distributing copies of those files with an access control-for surely the effort to create the former is more than the latter and more worthy of protection but has never been given it. As such electronic formats of Public Domain works do not fall under the DMCA and are exempt from the prohibitions of circumvention in section 1201.

Furthermore, the question that one can control access to a work in the Public Domain has no legal or historical precedence supporting it. One has always been able to reproduce books, sheet music, piano rolls, films, phonograph recordings of works in the public domain without having to cope with archaic access controls. Counter arguments based upon economics or marginal profits for production and distribution of works in the public domain have been held previously irrelevant by the courts and are even more so today given how scanning and optical character recognition have replaced the printers typebox. Other arguments that public domain works distributed with access controls should be protected under the DMCA because they might “compromise” copyrighted works that are distributed with the same access control are specious.

Additional Information/Documentation

None

2. Descriptive Name Class : Information collected by “Spyware” software that is encrypted or “Spyware” software whose operation uses encryption to hide its operation

Summary:

Commercially distributed software that is distributed with the intention of gathering information on users surreptitiously without their knowledge or consent is called “Spyware” by computer security specialists. While obstensively the Spyware program is distributed to perform one function, it is actually a Trojan Horse collecting information about the user of the software without their knowledge and relaying it back to the distributer of the software. It uses the same technology and means of distribution as computer viruses. The only difference is that Spyware is less malicious than many computer viruses which may collect passwords and credit card numbers to commit fraud. Computer viruses may use encryption to change their appearance and hide their true operations. Spyware also uses encryption to hide the information collected, transmitted, or to prevent reverse engineering of the code to determine just what it truly is doing. Since Spyware is a computer program it is also a copyrighted work that may also claim to be using encryption to control access to its workings or as a part of a copy protection “technology.” The prohibition on circumvention affects the ability of computer security specialists to determine what is or is not Spyware and what information has been compromised.

Facts and evidence:

In 2000, a company called Digital Convergence distributed a product called :CueCat. This was a free barcode reader with software for Windows or Macintosh that would allow one to scan in the barcodes of items purchased and be connect to a webpage for that product. The scanner was available at Radio Shack stores, could be requested through the mail, and even distributed in magazines such as Forbes and Parade. Registration could be on-line, throught the mail, or at a Radio Shack store. One could even get up to 5 registration numbers for members of the family. Intially things went well aside from a security breach at the Digital Convergence website which compromised users registration information. Several commentators wondered if :CueCat scanning could become obsessive for some people, or what benefit a :CueCat scanner really provided. There was one community of people who were able to answer those questions.

Digital Convergence did not provide LINUX software. As a consequence, several LINUX programmers decided to develop their own and reverse engineered the :CueCat. The programmers added the capability to not only scan items but construct a database of items one had scanned and their descriptions. In the course of the reverse engineering the scanner the LINUX programmers found that the transmissions were encrypted. Fortunately the scheme was trivial to break. What they discovered was that each :CueCat scanner had a unique identification number. When the :CueCat scanner was used, that identification number was transmitted to Digital Convergence. Digital Convergence was constructing a database of items purchased, probable dates, who purchased them and associating that with names, address, and even family members[2] without their knowledge[3]. This database was to be used for “data mining” for market demographics. Since the fact that their registration database was compromised, it is problematical whether this other database would be compromised since the company went bankrupt. :CueCat was one of the most colossal failures as Spyware but it does illustrate many of the common aspects. The victim was given a Trojan Horse. The actions of the Spyware were hidden because of the complexity of software and encryption. Communications was secret. These are also the tactics of computer viruses. While the effects of :CueCat were limited by the number of bar-code scanners distributed, another Spyware program was not.

The “granddaddy” of all spyware programs was called Aureate (which later changed its name to Radiate) which provided a Radiate Software Developers Kit that could embed advertising in software which "...collects voluntary demographic data that advertisers can use to target audiences" with "Precise audience targeting - Rich media - The ability for advertisements to be viewed even when users are not connected to the Internet - Splash screens - Dynamic messaging - Customized demographic collection - Real-time surveys". This toolkit was used in the development of hundreds of free Spyware software (from which Radiate received royalties). What the owners of over 30 Million computers that this software was installed did not know that it was installed secretly. It used the computer’s Internet connection without the owners knowledge. It hid itself on the computer and would not be deleted from the computer even if the Spyware application was uninstalled. It operated only when the keyboard or mouse were being used so that the user would not notice. Even two years later, it is not clear just what information the Aureate/Radiate did gather[4]. The well known computer security consultant, Steve Gibson spent 200 hours analyzing an early version of Aureate/Radiate and still was not certain what information was being gathered and transmitted although he was certain that Aureate/Radiate does cause system and web browser “crashes.” At this time there are over 850 known Spyware programs, many of which use the Aureate/Radiate toolkit even thought the company that created it is now defunct.

While the Aureate/Radiate is not available anymore, a successor called Web3000 is. This program replaces operating system components of windows with their own[5]. Registering the software embedded with Web3000 will not cause it to cease transmitting information back to their website but uninstalling it incorrectly can cause system problems.

[2] The only possibly relevant explanation I was able to find in the :CueCat, I “leased” was the following sentence in the “licensing terms” in a “clickwrap” window during installation: “Both the :CueCat Reader and the CRQ software are serialized to provide aggregated usage statistics and prevent technological theft.” In retrospect, “aggregated usage statistics” is clearly duplicitous.

[3] http://www.flyingbuttmonkeys.com/foocat/ and http://zdnet.com.com/2100-1107-524352.html

[4] Further discussion can be found at http://crc.com/oo/aureate.htm.

[5] Most notably Winsock32.dll which is a critical component for network access.

In addition to collecting information, some Spyware has been used to hijack the users own computer. One company called Brilliant Digital installed their own software in the popular free program KaZaA. This "parasite" program runs in the background using the idle micoprocessor time and disk space of the computer to create a private network called Altnet to create video and 3-D animation for advertisers. Of course, this slows down the users computer, their internet connection, and clutters up their disk with Brilliant Digital files. In another industry this would be called theft of service.

Having shown something of the nature of Spyware, what are some of the "tricks" that it uses. One spyware program called Comet Cursor uses encryption on the data transmitted[6]. Another program called STARR PC & Internet monitor logs keystrokes, passwords, keeps records of websites visited etc and stores all of this in a password protected encrypted file that can be emailed to another PC[7]. KeySpy records keystrokes into an encrypted and hidden disk file. HackerWacker also stores encrypted data and log files. ISpynow does all of this and uses encryption to permit access to the installed "iSpynow Control panel from a remote location"

Perhaps one of the most egregious pieces of Spyware is called DSSAgent and was distributed by Mattel corporation in a number of their childrens CD games including the popular Barbie, Carmen SanDiego, Reader Rabbit, and MYST. This same Spyware was used in Compton's Encyclopedia, National Geographic, and other programs such as 3D Home Architect, 3D Home Design by Broderbund[8]. The best decription of DSSAgent is by Simson Garfinkel "I fired up some tools and started pulling apart the DSSAgent program. I discovered that the DSSAgent contained a copy of the developer's kit for the Pretty Privacy encryption system, that it contained the ability to send e-mail and post forms to Web pages and that its creators had gone to great lengths to hide the software's function. And there was no copyright message indicating who had written the program."[9]

Argument:

The investigation of Spyware is adhoc and undertaken by individuals on their own time[10] since the makers of anti-virus software do not include Spyware programs in their databases and scan for them. Encryption is generally used to hide information rather than to control access to it. So confronted with possible spyware the investigator has several

[6] http://www.cometcursor.com

[7] For further information on many Spyware programs see http://www.modemspy.com/en/remote-computer-monitoring/

[8] When I discovered this while doing the research for these comments, I realized the Spyware I removed from my machine several months ago had been part of Broderbund 3D Home Design.

[9] http://dir.salon.com/tech/col/garf/2000/06/15/brodcast/index.html

[10] One less amusing incident that took place this year is that during its installation, one Spyware program called RadLight searched for installed components of the popular freeware firewall ZoneAlarm and a freeware Spyware scanner called Ad-aware and deleted them without the users knowledge. Not only does this allow RadLight to operate but also compromises the computer security leaving it vulnerable to other attacks by other programs or computer virus should they occur.

questions to address. Is the encryption used to protect privacy for users who know they are sending information? Or is the encryption used to prevent others from finding out what information is being sent? Or is the encryption being used to prevent others from reverse engineering some trade secret by controlling access to the executable code? Or is the encryption being use to hide the actual piece of spyware code as a polymorphic virus does[11]. Unlike computer viruses, Spyware is a Trojan Horse using a copyrighted work as "bait."Under the Digital Millenium Copyright Act, the Trojan Horse is also a "shield" since the encryption is an access control to copyright material. The DMCA can prevent the dissemination of knowledge by investigators. It can prevent the posting of preliminary code that circumvents the "access control".[12] What is disturbing with several of the Spyware programs discussed above is that in most instances the actual information that has been transmitted is still not known. Without the exemption to circumvent the "access control" to suspected spyware, the determination of effects of actual spyware cannot be completed.

Additional Information/Documentation

None

[11] A computer virus that uses encryption to change its "signature" between infections is called a polymorphic virus. It is not clear at this time how much of that technology has transferred to the "Spyware Industry". It is only clear that the technology that enables polymorphic viruses is present in many Spyware programs but the extent is undetermined

[12] This is not a theoretical argument. Professor Felton of Princeton University has already experienced this. The programmers that reverse engineered the :CueCat also were threatened with lawsuits.