Digital Rights Management: The Cost to Consumers

By AMBER SAMI KUBESCH
School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853 USA
(e-mail: adm234@cornell.edu)

STEPHEN WICKER
School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853 USA
(e-mail: wicker@ece.cornell.edu)

I. TOPIC DESCRIPTION AND IMPORTANCE

Copyright holders have worked to combat piracy through the use of digital rights management (DRM) systems designed to be increasingly more difficult to break. Along with these protections, however, have also come increased restrictions that can limit the ability of users to enjoy purchased content in ways otherwise permitted under fair use. Code-based restrictions implemented in DRM systems give copyright holders the technological ability to limit fair use rights further than allowed under Copyright Law—skewing the laws in their favor [1], [22], [28], [68], [69], [71].

In addition to reduction of fair use rights, users also face a loss of privacy due to DRM technologies that collect, store, and share user data. Types of information being collected include location data, system configurations, timestamps of when content is accessed, and sometimes even more personal types of data such as contact lists. Additionally, several companies have been found to correlate these data with other user information such as IP addresses, user IDs, gender, and age in order to analyze end users [26], [37], [41], [61], [65], [77], [78]. This process of collecting user data and sending it to remote servers is often done without the knowledge of the user, posing considerable concern.

DRM systems combined with the anti-circumvention legislation of the Digital Millennium Copyright Act (DMCA) put users at risk of losing the ability to enjoy fair use and other users rights. We cannot count on content distributors to be honest, considerate, accountable, or transparent; instead we must seek to rebuild a framework under which

Digital Object Identifier: 10.1109/JPROC.2015.2418457

the rights of users can be reclaimed and balanced against the needs of content providers.

This paper begins with a brief overview of how DRM technologies are being used to limit consumer rights. Next we show how this code is combined with a legal component, including the use of contractual agreements, to further narrow user rights. Providing a summary of the legal history, we build up to the current legal environment surrounding DRM in the United States, showing the need for DRM policy and coding changes to better balance the interests of copyright holders and the public.

II. CODE CONTEXT: HOW DRM LIMITS FAIR USE AND OTHER CONSUMER RIGHTS INCLUDING PRIVACY

To show why there is a pressing need for a form of DRM that incorporates fair use and other consumer rights, we share several ways in which DRM currently imposes on them. We look at other actions taken through DRM such as invalidating or removing access to purchased content, retroactively restricting DRM privileges after purchase, reducing user privacy by collecting and transmitting personal information through processes that "phone home," and malware-like tactics used to control users' systems.

One issue with DRM protected content is that of renewability, or the ability of content controllers to delete or alter available features after purchase. An ebook seller, Fictionwise, used a third-party supplier of DRM encrypted ebooks, Overdrive, to supply approximately 300 000 electronic book titles to its users. Providing only 30 days of warning to customers, Overdrive's servers were shut down on January 30, 2009. Files already downloaded continued to work, but the purchases became invalidated; as a result, content could not be transferred to a new device or replaced if the original file was lost or deleted. Fictionwise stated in their FAQs online that "Fictionwise strives to maintain your purchases indefinitely, but our terms of service do not guarantee they will be available forever. Forever is a long time. [. . .] We do not have legal control of those third party servers. If those third party servers 'go dark' for one reason or another, we have no way to continue delivering those files. It is important to note that other ebook retailers such as Barnes and Noble, Gemstar, and Amazon.com's original ebook store circa 2004 did not make any effort to maintain long term customer access to purchased material when they shut down their ebook operations in the past. They announced a time period for final download then shut down the servers" [15], [21], [72].

Ebook users faced another issue with renewability when Amazon deleted copies of George Orwell's *1984* and *Animal Farm* as well as some works of Ayn Rand from users' Kindles, rendering user-added notes and annotations associated with those files useless [70], [72]. Amazon refunded the purchases, but left users angry that the company had the ability to retroactively modify user access to purchased content.

Short of removing entire works, some users experience changes in DRM privileges after purchasing content. The Author's Guild fought to force Amazon to block text-to-speech privileges on a title-by-title basis from the Kindle [4], and Amazon ultimately agreed to remove the functionality from already purchased titles on users' devices at the request of publishers [72].

This issue is not confined to ebooks; consumers of music and video games have faced similar losses. In 2008, music services offered by MSN, Yahoo! Music, and Walmart Music announced that they would be shutting down their DRM servers and that users would no longer be able to transfer songs to new devices or access purchased content after changing operating systems. Customer reactions caused MSN and Walmart to announce a delay in their shutdown date and Yahoo! to offer compensation to their customers [15]. Users of Apple's iTunes service have also experienced DRM privilege restrictions. Prior to April 2004, the iTunes music store allowed users to burn purchased music on up to ten CDs. Apple later issued an update to iTunes reducing that limit to only seven allowable copies [14].

Another consumer cost of DRM is loss of privacy. DRM has "the potential to facilitate an unprecedented degree of surveillance of consumers' reading, listening, viewing and browsing habits" [5]. This may be even more intrusive in the mobile realm, where "smartphones are often on and tethered to their user, transmitting rich data to the app developers. Users of mobile devices are vulnerable to privacy intrusion and abuse by numerous entities, app developers, analytic services, and advertising networks. These entities could have access to sensitive information, including a user's location, contacts, identity, messages and photos" [57]. A *Wall Street Journal* investigation found that "these phones don't keep secrets. They are sharing this personal data widely and regularly" [78].

In fact, some users reported to have run tests discovering that several Pinch Media enabled iPhone apps were storing and sending back to Pinch Media's servers ("phoning home") combinations of the following data: the unique device identifier; iPhone model; OS version; app version; if the iPhone running the app was jailbroken; if the copy of the app had been pirated; the times and dates when the app was opened and closed; latitude and longitude of the iPhone; and—if Facebook enabled—the gender, birth month, and day of the user [41], [61]. Flurry Analytics, which has since merged with Pinch Media, admits in their privacy policy that they collect the following data: "User ID (for your service), latitude and longitude (obfuscated by Flurry to state/city), gender, age, events, errors, and page views. Finally, we see the IP

address, device type, locale and timezone of the user through the HTTP request" and may also provide the app developer with the ability to collect raw data from Flurry including the "timestamp, platform, event, and user ID" [26]. Cofounder of Pinch Media, Greg Yardley, responded to outrage over the discovery that Pinch Media enabled apps were phoning home by saying, "Every single person who installs an iPhone application consents to data collection in advance—it's right there in the default EULA Apple's provided so developers don't have to hire lawyers before publishing something."[1] While many times not transparent to users, these activities may indeed be allowed by the EULA, although often in vague, nonlimiting terms. There are many other analytics companies like Flurry, including Medialet and Mobclix, but it is often not known to users that some of their apps are running analytics software, which ones are collecting these data, or the scope of data being obtained [37], [53], [55], [78].

Although analytics companies defend this process as one in which no personally identifiable information is collected, the practice of collecting a device's unique identifier means that they are able to track users over time. Unlike cookies, this is built into the device and cannot be cleared [78], [89]. One user wrote in response to Pinch Media that "As far as not having personally identifiable information, the fact is that as soon as I use an app that requires registration of my name or email address, then my [unique device identifier (UDID)] could be associated with my identify by the developer of this app. What's to stop you from gathering this information from developers? Even if you don't have my name, the [(UDID)] might as well be my name" [41].

Apps like Facebook,[2] Hipster, and Path, and about a dozen others were found to be uploading user's contact lists to their servers in a move later defended by Path as being an industry standard practice [33], [34], [56], [65], [77], [89]. Seven popular mobile games created by Storm8 were also criticized for sending home users' phone numbers, unique device identifiers, and e-mail addresses, all unencrypted in plain text [6], [29]. Programs downloaded from an app store are not the only ones potentially collecting user data, however. One developer discovered that the WebOS side of his Palm Pre device "periodically uploads information to Palm, Inc" [32], including location data and application usage. Carrier IQ, software installed on 150 million phones by cell phone companies, was found to be recording keystrokes, location data, browsing history, application use, battery use, and radio activity [11], [13]. Possibly the result of an error, it was also found "that keystrokes, text message content and other very sensitive information is in fact being transmitted from some phones on which Carrier IQ is installed to third parties" [11].[3] Finally, while users may feel comfortable and let their guard down when using iPhone's Siri feature, they should keep in mind that it collects user data in order to have a better context for the spoken commands and that Apple reserves the right to retain both voice inputs and user data for their own uses as well as those of their subsidiaries [2].[4]

Along with contact lists, it is also possible for mobile apps to access and copy entire photo albums without the user's knowledge or explicit opt-in, as found on both Apple and Android devices [7], [8]. Black Hat researcher, Nicolas Seriot, developed a proof-of-concept iPhone app that was able to collect and send home the following data: phone number, address book contents, recent Safari searches, YouTube history, e-mail account data including full name and e-mail address, unique device identifier, SIM card serial number, and International Mobile Subscriber Identity [73]. Spyware under the name of FinFisher was found to be able to "secretly turn on a device's microphone, track its location and monitor e-mails, text messages, and voice calls" [74] on a range of mobile devices including the iPhone and BlackBerry.[5] While these examples show what technology is currently possible in the realm of mobile devices, these activities may be illegal based on current EULAs. However, it raises the question of how far companies could take the terms in their user agreements. Certainly a line must be drawn beyond which courts in the United States would consider

[1]This quote from Greg Yardley was originally found as a comment to an article posted online at http://gadgets.boingboing.net/2009/04/13/pinch-media-statisti.html#comment-463496). We verified with him via e-mail communication on November 12, 2013 that it was his comment.

[2]Facebook has recently come under fire for another method of data collection through the use of Atlas, an advertising platform for tracking user behavior that "lets advertisers target you across all of your devices and on participating websites, based on characteristics from your Facebook profile such as age, gender, and location. It will also attempt to track the products you buy both online and off." With no way to opt out of data collection, "Atlas uses the advertising industry's phony definition of 'opt out,' which has the unfortunate characteristic of meaning 'pretend not to track' and offers no privacy benefits whatsoever. While you may think you are opting out of a large data collection scheme by, as Atlas expects you to do, accepting an opt out cookie, the platform will merely stop serving you targeted ads." Facebook noted that many of the complaints director toward them for this move are actually industry-wide issues [12].

[3]Security researcher Trevor Eckhart, who discovered the Carrier IQ rootkit software, was sent a Cease & Desist notice from Carrier IQ citing copyright infringement and demanding "that Eckhart turn over contact information for every person who had obtained the files from him, and that he replace his analysis with a statement—written for him by Carrier IQ—disavowing his research" [39]. Ultimately the Electronic Frontier Foundation took up his case and concluded "that Carrier IQ's real goal [was] to suppress Eckhart's research and prevent others from verifying his findings," one risk of abuse of the Digital Millennium Copyright Act.

[4]Spyware-like tactics of data collection are now a concern for eBooks as well. The Electronic Frontier Foundation recently learned that "two independent reports claim that Adobe's e-book software, 'Digital Editions,' logs every document readers add to their local 'library,' tracks what happens with those files, and then sends those logs back to the mother-ship, over the Internet, in the clear." Adobe later admitted to collecting information about which books users are currently reading, where the book is being read, how long the user has been reading it, and how much has been read [54].

[5]This is not just a worry for the future; some Android and iPhone apps from their respective app stores have already been found to secretly activate cell phone microphones, including *Color*, *Shopkick*, and *IntoNow* [16], [65].

such terms to be unreasonable, unconscionable, and ultimately illegal.

The phenomenon of protected content collecting personal data and "phoning home" is not limited to mobile apps. In 2005, it was discovered that Song-BMG's copy-protected CDs were transmitting personal information without the user's knowledge or consent [31]. Specifically, the DRM systems implemented by Song-BMG "were designed to contact a vendor Web site whenever the user inserted a protected disc. The ostensible purpose of this was to download images or advertisements that would be displayed while the music played, but it also created entries in the vendor's Web server log, noting the users' IP addresses, disc inserted, and the times and dates it was inserted" [25]. The discs also performed undisclosed installation of software onto consumer's computers. The discs shipped with two versions of DRM: one was a rootkit that cloaked its presence by modifying the system to hide the fact that it was running and to make it challenging to remove; the other resisted detection and removal, installing itself even if the user declined the terms in the EULA. Researchers Halerman and Felten concluded that their case study on Song-BMG revealed "similarities between DRM and malicious software such as spyware, the temptation of DRM vendors to adopt malware tactics, the tendency of DRM to erode privacy, the strategic use of access control to control markets, the failure of *ad hoc* designs, and the force of differing incentives in shaping behavior and causing conflict" [31].

Another complaint with the tactics used by Song-BMG was that of limited portability. After purchase, users learned that they were limited by the number of digital copies of the material that they could create, that they had to use Sony's proprietary media player to play the content on their computers, and that they were not permitted to convert music to common digital formats such as that used by iTunes. Ultimately this meant that the files were only compatible with Sony and Microsoft portable players and unusable with other devices like the iPod. The investigations of Song-BMG copy-protected disks revealed several ways in which content owners do not make limitations transparent to users before purchase. Here, consumers were only made aware of portability issues after inserting the disks into their computers and were unaware that Sony's media player would be serving advertisements while they played their paid content [50].

Consumers of ebooks also often do not know what limitations they will face until after they have purchased content. They may be surprised to learn that features such as read-aloud and use with third party programs can be disabled on a title-to-title basis. While this may be a minor inconvenience to some users, it poses a bigger problem for those with disabilities who rely on those features in order to make use of the content, such as those who need the use of an included read-aloud function or the ability to interface with third party software that can do so [72]. "The advent of digital technology makes it easier than ever for disabled people to enjoy the same media as people without disabilities. A digital book can be read aloud by a blind user's computer, sparing her the need to wait until [a] volunteer can be found to record an audio version. Indeed, for the first time the blind can enjoy newspapers at the same time as the sighted, simply by 'reading' them through a Web-browser that reads the articles aloud to them, or exports them via a Braille terminal. [. . .] However, DRM systems stymie these activities. Adobe's ebooks come with the capacity to be read aloud by a computer, but allow authors to switch this capability off. Other ebook technologies lack this capability altogether, and actively prevent interoperability with third party software such as text-to-speech programs" [14].

DRM code is able to limit access and interoperability, locking consumers out of expected functionality or that which could be offered through third-party vendors. "In a few words, the restrictions imposed by technological measures are frequently unclear to consumers. This lack of information can induce consumers to make buying decisions which they would not have made had they been better informed" [50]. In order to maintain fairness where DRM is used, these limitations should be disclosed before purchase to enable consumers to make informed buying decisions.

Digital restrictions like these combined with anti-circumvention legislation have been criticized for limiting or removing fair use rights. Passed in 1998, the Digital Millennium Copyright Act (DMCA) made the circumvention of copyright protection mechanisms illegal, with the temporary exception of a limited number of classes of works [48], [83]. One effect of the DMCA has been to narrow fair use rights further than the provisions made in law for copyright holders. Succinctly, "Copyright owners can effectively eliminate fair use by utilizing DRM systems sanctioned under the DMCA and litigating against anyone who tampers with those measures. Thus, re-writing the copyright fundamentals developed by Congress and courts over more than a century" [71].

III. LEGAL CONTEXT

In this section, we show examples of terms being included in EULAs such as those prohibiting users from engaging in class-action lawsuits, requiring that users allow collection of their personal data, and even those that force users to relinquish fair use rights. Several case studies in the United States are presented and compared to the way similar agreements are handled in the European Union (EU). The EU has established fundamental consumer rights and taken action against companies that require EULAs with unconscionable terms; in the United States, although several legal attempts have been made to limit the ability of contractual agreements to force users to waive rights they would otherwise have enjoyed under copyright law, we have not seen the same success in this area as Europe.

The current legal environment in the United States is perceived by many to be skewed unfairly in favor of copyright holders. In addition to code-based restrictions imposed on users by DRM technology, further rights can be taken away through licenses and contracts, such as End User License Agreements (EULAs) [10], [14], [15], [28], [49], [51], [68], [69], [71].

As of this writing, some EULAs include terms to prohibit users from participating in a class-action lawsuit or to require users to allow collection of their personal data. Consenting to the Sony Playstation Vita System of Software License Agreement (Version 1.1) [75] or a recent PayPal User Agreement [63], for example, means that the user waives the right to engage in a class-action lawsuit against the company—unless a written notification requesting the retention that right is sent within 30 days of accepting the agreement. Facebook retains the right to log and use data on users including IP addresses, the date and time of all logins and logouts, messages sent between users, a history of conversations through Facebook Chat, all notifications and whether the user had e-mail and text enabled or disabled for each, any photos uploaded to a Facebook account (presumably even those later deleted), as well as a history of other sites visited. Facebook is only one of many services that collect user data.

The Electronic Frontier Foundation warns that "Companies have a lot of leeway about what goes into the privacy policy. They can use vague, overbroad language so they can collect lots of data about users, share it with affiliates, sell it to marketers, or provide it to the government upon request. And even a strong privacy policy is little consolation; a privacy policy can change at any time, so today's protective language could be tomorrow's permissive exceptions" [38]. Considering that most Americans believe that their information is being kept private when they see the term "privacy policy" [79], that the common attitude of consumers toward EULAs is to select that they agree without reading the terms [89], and that the terms in these contracts are unilaterally determined and dictated, users today find themselves in a very poor position with respect to the companies drafting these license agreements.

The European Union has established some fundamental consumer rights and taken action against companies that require EULAs with "unconscionable" terms. Some terms that have been argued to be unfair include those that allow the copyright holder to modify the agreement without notice, to change the rights restrictions on already purchased files, to limit interoperability with other software or devices, to disclaim responsibility for any viruses or other damage that could result to the user's computer system through use of their services or products, along with other misleading or unfair behavior including terms users likely would have refused had they understood what was included [27], [50].

In the United States, however, EULAs in the form of click-through or shrink-wrap agreements are being upheld in courts (although not consistently). A high profile case illustrating this was that of Blizzard vs. bnetd.org. Vivendi-Universal's Blizzard Entertainment alleged that software created by bnetd.org allowing users to play Blizzard games over the Internet was only made possible by the defendant's use of reverse engineering, a violation of Blizzard's ELUA. A court ruled in 2005 that even if this would have fallen under fair use, bnetd.org waived that right by agreeing to Blizzard's ELUA [15], [84].

Even though some legal attempts have been made to limit the ability of contractual agreements to force users to waive rights they could have otherwise enjoyed under Copyright Law, the United States has not seen the same success in this area as Europe. In 1997, Rep. Boucher introduced the Digital Era Copyright Enhancement Act (105th Congress Bill H.R. 3048) to Congress as an alternative to the restrictive proposals under the DMCA; however, it died after being referred to a subcommittee in 1998, ultimately losing out to the DMCA proposal. Some of the major differences between H.R. 3048 and the DMCA include that the former took fair uses into consideration by only prohibiting the alteration or removal of DRM restrictions when done for the purpose of infringement. Further, H.R. 3048 would have prohibited the ability of copyright owners to limit fair use rights through shrink-wrap or click-through agreements [5], [46], [47].

Another bill proposed to establish greater consumer rights with respect to DRM, The Consumer, Schools, and Libraries Digital Rights Management Awareness Act of 2003, was introduced by Senator Brownback and supported by the U.S. Public Policy Committee of the Association for Computing Machinery (USACM). Among the terms proposed were to promote greater public transparency when DRM is used to protect digital content, greater privacy rights for users, and prohibitions on the government from mandating the use of any specific copy-protection technologies. This bill also died in Congress.

"Pro-digital-consumer legislation has enjoyed no great success in U.S. The most famous consumer-rights legislation proposed in the recent time, the Digital Media Consumers' Rights Act (DMCRA), has been introduced into Congress three times without success" [50]. First introduced in 2003, the goals of DMCRA were to restore fair use rights to users by allowing the circumvention of copy protection measures for the purpose of scientific research or when "such circumvention does not result in an infringement of the copyright in the work" [44]. It would have also allowed the distribution of hardware and software enabling such circumvention if there existed a "significant noninfringing use" for the technology. It would have also required greater transparency of limitations through the clear labeling of copy-protected compact discs.

Nations take different approaches to privacy protection, ranging from a "strong 'rights-based' approach [as]

embodied in the [EU] Data Protection Directive, to the US preference for relying on market forces rather than the law to protect personal information" [49]. The United States is one of 21 member economies of the Asia-Pacific Economic Cooperation (APEC) that have agreed to the APEC Privacy Framework in order to create region-wide compatibility of privacy policies and data flow [4]. "The significance of the twenty-one APEC economies adopting common information privacy standards cannot be doubted. The APEC economies are located on four continents, account for more than a third of the world's population, half its GDP, and almost half of world trade" [30].

One complaint with APEC Privacy Framework is that it allows collected data to be used for any "compatible or related purposes" and does not suggest that collection should be the least necessary. Although APEC member nations can implement stronger regional laws, doing so seems to be discouraged: the forward to the Framework states that "Member Economies, consistent with the APEC Privacy Framework and any existing domestic privacy protections, should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers" [4]. Showing a preference for allowing data flow over protecting privacy, "The Preamble speaks of 'ensuring' free flow of information but only of 'encouraging' privacy protection. The final points in the Preamble refer to free flow of information as 'essential,' but do not accord this status to privacy protection. These examples of terminology indicate how the Framework has a bias against privacy protection in favor of free flow of information" [30].

IV. CONCLUSION

DRM is used to mitigate the losses content owners face due to piracy, but this technology also enables copyright holders to overreach their rights and narrow those of consumers. The current legal and technological landscape shows that we cannot rely on market forces alone to find a fair balance between the rights of users and those of copyright holders. Policy changes and encouraging principles of good DRM design—including maintaining transparency, using DRM only to reinforce existing copyright laws without adding further restrictions, and collecting personal information only as necessary for the proper functioning of the DRM system—are needed in order to better balance the interests of copyright holder with those of users. We encourage legislators to safeguard users' rights by developing a legal backing to protect them. We also encourage developers of DRM to remain mindful of the implications of their designs by carefully considering the impact their technology has on consumer rights, including fair use and privacy. ■

REFERENCES

[1] A. W. Appel and E. W. Felten, "Technological access control interferes with noninfringing scholarship," *Commun. ACM*, vol. 43, no. 9, pp. 21–23, Sep. 2000.

[2] Apple, Inc., *iOS Software License Agreement (EA0930)*, Oct. 8, 2012. [Online]. Available: http://www.apple.com/legal/sla/docs/ios6.pdf?

[3] Apple Inc., *Software License Agreement for iTunes*, Aug. 23, 2012.

[4] The Author's Guild, "Amazon reverses stance on computer-generated audio for the Kindle 2," Mar. 2, 2009. [Online]. Available: http://www.authorsguild.org/advocacy/articles/amazon-reversal-on-text-to-speech.html

[5] E. Becker, W. Buhse, D. Günnewig, and N. Rump, *Digital Rights Management: Technological, Economic, Legal and Political Aspects*. New York, NY, USA: Springer-Verlag, 2003.

[6] Y. Benjamin, *Apple Privacy Score: Snow Leopard—10, iPhone—0*, SFGate, Aug. 27, 2009. [Online]. Available: http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?blogid=150&entry_id=46236

[7] N. Bilton, "Apple loophole give developers access to photos," *The New York Times*, Feb. 28, 2013. [Online]. Available: http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/

[8] B. X. Chen and N. Bilton, "Et Tu, Google? Android apps can also secretly copy photos," *The New York Times*, Mar. 1, 2012. [Online]. Available: http://bits.blogs.nytimes.com/2012/03/01/android-photos/

[9] D. S. Chisum, T. T. Ochoa, S. Ghosh, and M. LaFrance, "Understanding intellectual property law (2nd edition)," *LexisNexis*, 2011.

[10] J. E. Cohen, "DRM and privacy," *Commun. ACM*, vol. 46, no. 4, pp. 46–49, Apr. 2003.

[11] P. Eckersley, "Some facts about carrier IQ," Electronic Frontier Foundation, Dec. 13, 2011. [Online]. Available: https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture

[12] P. Eckersley and A. Kamdar, "Facebook increases its tracking reach with Atlas, and users have little choice about it," Electronic Frontier Foundation, Oct. 2, 2014. [Online]. Available: https://www.eff.org/deeplinks/2014/10/facebook-increases-its-tracking-reach-atlas-and-users-have-little-choice-about-it

[13] T. Eckhart, "CarrierIQ," *Android Security Test*. [Online]. Available: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[14] Electronic Frontier Foundation, "Digital rights management: A failure in the developed world, a danger to the developing world." [Online]. Available: http://w2.eff.org/IP/DRM/drm_paper.php

[15] Electronic Frontier Foundation, "FTC town hall: Digital rights management technologies," Mar. 2009. [Online]. Available: www.eff.org/files/filenode/DRM/DRMCOMMENTS_final.pdf

[16] M. Elgan, "Snooping: It's not a crime, it's a feature: New apps hijack the microphone in your cell phone to listen in on your life," *Computer World*, Apr. 16, 2011. [Online]. Available: http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature

[17] Epic Games, *Gears of War Official Forums*. [Online]. Available: http://forums.epicgames.com/threads/656177-quot-You-cannot-run-the-game-with-modified-executable-code-quot-WTF-help-please!/page3

[18] J. S. Erickson, "Fair use, DRM, and trusted computing," *Commun. ACM*, vol. 46, no. 4, pp. 34–39, Apr. 2003.

[19] Facebook, "Accessing your Facbook info." [Online]. Available: https://www.facebook.com/help/326826564067688

[20] U.S. Federal Trade Commission, "Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers," FTC Rep., Mar. 2012. [Online]. Available: http://ftc.gov/os/2012/03/120326privacyreport.pdf

[21] Fictionwise LLC, "Overdrive and the eReader replacement file program." [Online]. Available: http://mobile.fictionwise.com/servlet/mw?t=help_Overdrive-Replacement-Faq.htm

[22] E. W. Felten, "A skeptical view of DRM and fair use," *Commun. ACM*, vol. 46, no. 4, pp. 56–61, Apr. 2003.

[23] E. W. Felten, "DRM and public policy," *Commun. ACM*, vol. 48, no. 7, p. 112, Jul. 2005.

[24] E. W. Felten, "Understanding trusted computing: Will its benefits outweigh its drawbacks?" *IEEE Security Privacy*, vol. 1, no. 3, pp. 60–62, May 2003.

[25] E. W. Felten and J. A. Halderman, "Digital rights management, spyware, and security," *IEEE Security Privacy*, vol. 4, no. 1, pp. 18–23, Jan./Feb. 2006.

[26] Flurry, "Privacy policy." [Online]. Available: http://www.flurry.com/privacy-policy.html

[27] Forbrukerombudet, "iTunes violates Norwegian law," Jul. 6, 2006. [Online]. Available: http://www.forbrukerombudet.no/id/11032467

[28] B. L. Fox and B. A. LaMacchia, "Encouraging recognition of fair uses in DRM systems," *Commun. ACM*, vol. 46, no. 4, pp. 61–63, Apr. 2003.

[29] D. Goodin, "Backdoor in top iPhone games stole user data, suit claims," *The Register*, Nov. 6, 2009. [Online]. Available: http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/

[30] G. GreenLeaf, "APEC's privacy framework sets a new low standard for the Asia-Pacific," in *New Dimensions in Privacy Law: International and Comparative Perspectives*, A. T. Kenyon and M. Richardson, Eds. New York, NY, USA: Cambridge Univ. Press, 2006, pp. 91–120.

[31] J. A. Halderman and E. W. Felten, "Lessons from the Sony CD DRM episode," in *Proc. USENIX Security Symp.*, Aug. 2006, pp. 77–92.

[32] J. Hess, "Palm pre privacy." [Online]. Available: http://joeyh.name/blog/entry/Palm_Pre_privacy/

[33] P. Higgins, "A better path for apps: Respecting users and their privacy," Electronic Frontier Foundation, Feb. 8, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/02/better-path-apps-respecting-users-and-their-privacy

[34] P. Higgins, "Highlighting a privacy problem: Apps need to respect user rights from the start," Electronic Frontier Foundation, Mar. 8, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/03/highlighting-privacy-problems-apps-need-respect-user-rights-start

[35] P. Higgins, "Mobile user privacy bill of rights," Electronic Frontier Foundation, Mar. 2, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights

[36] P. Higgins and L. Tien, "EFF to FCC: Consumers face uphill battle in fight for mobile device privacy," Electronic Frontier Foundation, Jul. 16, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/07/eff-fcc-consumers-face-uphill-battle-fight-mobile-device-privacy

[37] P. Higgins and L. Tien, "Privacy and security of information stored on mobile communications devices: CC Docket No. 96-115; DA 12-818 (77 Fed. Reg. 35336)," Electronic Frontier Foundation, Jul. 13, 2012. [Online]. Available: https://www.eff.org/files/EFF%20FCC%20Mobile%20Privacy%20Comments.pdf

[38] P. Higgins and R. Reitman, "California AG agreement calls on mobile apps to be transparent about all the ways they invade user privacy," Electronic Frontier Foundation, Feb. 23, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/02/california-ag-agreement-calls-mobile-apps-be-transparent-about-all-ways-they

[39] M. Hofmann, "Carrier IQ tries to censor research with baseless legal threat," Electronic Frontier Foundation, Nov. 21, 2011. [Online]. Available: https://www.eff.org/deeplinks/2011/11/carrieriq-censor-research-baseless-legal-threat

[40] M. Hofmann, "Obama Administration unveils promising consumer privacy plan, but the devil will be in the details," Electronic Frontier Foundation, Feb. 23, 2012. [Online]. Available: https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-devil-details

[41] H. Holtmann, "Is big brother listening in on many iPhone apps?" Eidac, Mar. 10, 2009. [Online]. Available: http://www.eidac.de/?p=109

[42] L. Lessig, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. Baltimore, MD, USA: The Penguin Press, 2004, 348 pages.

[43] L. Lessig, *Code Version 2.0*. New York, NY, USA: Basic Books, 2006.

[44] Library of Congress, *Bill Text 108th Congress (2003–2004) H.R.107.IH*. [Online]. Available: http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:

[45] Library of Congress, *Bill Text 108th Congress (2003–2004) S.1621.IS*. [Online]. Available: http://thomas.loc.gov/cgi-bin/query/z?c108:s1621:

[46] Library of Congress, *Bill Text Versions 105th Congress (1997–1998) H.R.2281*. [Online]. Available: http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281:

[47] Library of Congress, *Bill Text 105th Congress (1997–1998) H.R.3048.IH*. [Online]. Available: http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.3048:

[48] Library of Congress, "Exemption to prohibition on circumvention of copyright protection systems for access control technologies," Oct. 26, 2012. [Online]. Available: http://www.copyright.gov/fedreg/2012/77fr65260.pdf

[49] D. Lindsay and S. Ricketson, "Copyright, privacy, and digital rights management (DRM)," in *New Dimensions in Privacy Law: International and Comparative Perspectives*, A. T. Kenyon and M. Richardson, Eds. New York, NY, USA: Cambridge Univ. Press, 2006, pp. 121–153.

[50] N. Lucchi, "Countering the unfair play of DRM technologies," *Texas Intellectual Property Law J.*, vol. 16, no. 1, pp. 91–123, 2007.

[51] V. Mayer-Shönberger, "Beyond copyright: Managing information rights with DRM," *Denver Univ. Law Rev.*, vol. 84, no. 1, pp. 181–198, 2007.

[52] G. Mazziotti, "Freedom of use vs. DRM technology," in *EU Digital Copyright Law and the End-User*. New York, NY, USA: Springer-Verlag, 2008, ch. 7, pp. 179–229.

[53] Medialets, *Welcome to Muse*. [Online]. Available: http://muse.medialets.com

[54] C. McSherry, "Adobe spyware reveals (again) the price of DRM: Your privacy and security," Electronic Frontier Foundation, Oct. 7, 2014. [Online]. Available: https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security

[55] Mobclix, *Analytics*. [Online]. Available: http://www.mobclix.com/faqs.html#faqs-4

[56] D. Morin, *We Are Sorry*, Path, Feb. 8, 2012. [Online]. Available: http://blog.path.com/post/17274932484/we-are-sorry

[57] Office of the Attorney General, "Attorney General Kamala D. Harris secures global agreement to strengthen privacy protections for users of mobile applications," State of California Department of Justice, Feb. 22, 2012. [Online]. Available: http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy

[58] K. Opsahl, "A bill of privacy rights for social network users," Electronic Frontier Foundation, May 19, 2010. [Online]. Available: https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users

[59] The Organisation for Economic Co-operation and Development, "30 years after: The impact of the OECD privacy guidelines," Mar. 10, 2010. [Online]. Available: http://www.oecd.org/sti/ieconomy/30yearsafterthe impactoftheoecdprivacyguidelines.htm

[60] The Organisation for Economic Co-operation and Development (OECD), "OECD guidelines governing the protection of privacy and transborder flows of personal data, C(80)58/FINAL," Jul. 11, 2013. [Online]. Available: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[61] 0th3lo, "Pinchmedia: The anatomy of a spyware vendor," Jul. 31, 2009. [Online]. Available: http://archive-i-phone-home.blogspot.com/2009/07/pinchmedia-anatomy-of-spyware-vendor.html

[62] N. A. Ozer, "Note to self: Siri not just working for me, working full-time for Apple, too," American Civil Liberties Union of Northern California, Mar. 12, 2012. [Online]. Available: https://www.aclunc.org/blog/note-self-siri-not-just-working-me-working-full-time-apple-too

[63] PayPal, Inc., *Amendment to the PayPal User Agreement and Privacy Policy*, Effective Date: Nov. 1, 2012. [Online]. Available: https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=ua/US_20121001_Amendment_to_UA_and_Privacy_print&fli=true&locale.x=en_US

[64] S. Perez, "Dear iPhone users: Your apps are spying on you," *The New York Times*, Aug. 17, 2009. [Online]. Available: http://www.nytimes.com/external/readwriteweb/2009/08/17/17readwriteweb-dear-iphone-users-your-apps-are-spying-on-y-42589.html

[65] N. Perlroth and N. Bilton, "An easy sweep of user data from devices," *The New York Times*, Feb. 16, 2012. [Online]. Available: http://query.nytimes.com/gst/fullpage.html?res=9B07E4D7163FF935A25751C0A9649D8B63

[66] J. T. Rosch, "Keynote address: A different perspective on DRM," *Berkeley Technol. Law J.*, vol. 22, no. 3, pp. 971–980, 2007.

[67] B. Rosenblatt, "DRM, law and technology: An American perspective," *Online Inf. Rev.*, vol. 31, no. 1, pp. 73–84, 2007.

[68] C. Russell, "Fair use under fire," *Library J.*, vol. 128, no. 13, p. 32, Aug. 2003.

[69] P. Samuelson, "DRM {and, or, vs.} the law," *Commun. ACM*, vol. 46, no. 4, pp. 41–45, Apr. 2003.

[70] A. C. Sanders, "Restraining Amazon.com's Orwellian POTENTIAL: The computer fraud and abuse act as consumer rights legislation," *Fed. Commun. Law J.*, vol. 63, no. 2, pp. 535–552, Mar. 2011.

[71] D. J. Schaffner, "The digital millennium copyright act: Overextension of copyright protection and the unintended chilling effects on fair use, free speech, and innovation," *Cornell J. Law Public Policy*, vol. 14, no. 1, pp. 145–170, 2004.

[72] K. Schiller, "A happy medium: Ebooks, licensing, and DRM," *Inf. Today*, vol. 27, no. 2, pp. 42–44, Feb. 2010.

[73] N. Seriot, "iPhone privacy," *Black Hat*2010. [Online]. Available: http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf

[74] V. Silver, "Spyware matching FinFisher can take over iPhones," *Bloomberg News*, Aug. 29, 2012. [Online]. Available: http://www.bloomberg.com/news/2012-08-29/spyware-matching-finfisher-can-take-over-iphone-and-blackberry.html

[75] Sony Computer Entertainment Inc., *Playstation Vita System Software License Agreement (Version 1.1)*, 2011. [Online]. Available: http://www.scei.co.jp/psvita-eula/psvita_eula_en.html

[76] R. Stim, *Getting Permission: How to License and Clear Copyrighted Materials Online and Off*. Berkeley, CA, USA: Nolo.com, 2000, book Collection (EBSCOhost).

[77] A. Thampi, "Path uploads your entire iPhone address book to its servers," Mclov.in, Feb. 8, 2012. [Online]. Available: http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html

[78] S. Thurm and Y. I. Kane, "Your apps are watching you: A WSJ investigation finds that iPhone and android apps are breaching the privacy of smartphone users," *The Wall Street J.*, Dec. 17, 2010. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602

[79] J. Turow, D. K. Mulligan, and C. J. Hoofnagle, "Research report: Consumers fundamentally misunderstand the online advertising marketplace," *Berkeley Law, Univ. California*, Oct. 2007. [Online]. Available: http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf

[80] U.S. Copyright Office, *Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code: Subject Matter and Scope of Copyright*, Circular 92. [Online]. Available: http://www.copyright.gov/title17/92chap1.html

[81] U.S. Copyright Office, *Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code: Copyright Protection and Management Systems*, Circular 92. [Online]. Available: http://www.copyright.gov/title17/92chap12.html

[82] U.S. Copyright Office, *Rulemaking on Exemptions From Prohibition on Circumvention of Technological Measures That Control Access to Copyrighted Works*. [Online]. Available: http://www.copyright.gov/1201/2010/

[83] U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary*, Oct. 28, 1998. [Online]. Available: http://www.copyright.gov/legislation/dmca.pdf

[84] U.S. Court of Appeals, *No. 04-3654: Vivendi Universal, Inc. v. Jung & Crittenden*, Jun. 20, 2005. [Online]. Available: https://www.eff.org/files/filenode/Blizzard_v_bnetd/20050901_decision.pdf

[85] U.S. Court of Appeals, *Second Circuit, Maxtone-Graham v. Burtchaell 803 F.2d 1253*, Oct. 15, 1986. [Online]. Available: http://www.studentweb.law.ttu.edu/cochran/Cases%20&%20Readings/Copyright-UNT/maxtonegraham.htm

[86] U.S. District Court for the District of New Hampshire, *Keep Thomson Governor Committee, Peter Thomson, Chairman, Orford, New Hampshire v. Citizens for Gallen Committee, Virginia Connors, Chairman, and Hugh Gallen*, Oct. 1978. [Online]. Available: http://law.onu.edu/sites/default/files/457_F__Supp__957%28rev%29%28DAK%29.pdf

[87] U.S. Government Accountability Office, *Report to Congressional Requesters: Privacy Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (GAO-08-536), May 2008.

[88] U.S. Public Policy Committee of the Association for Computing Machinery, *Letter to the Honorable Sam Brownback*, Feb. 2004. [Online]. Available: http://techpolicy.acm.org/blog/?p=17

[89] J. M. Urban, C. J. Hoofnagle, and S. Li, *Mobile Phones and Privacy: UC Berkeley Public Law Research Paper No. 2103405*, BCLT Research Paper Series, Jul. 2012.

[90] "The Journal's cellphone testing methodology," *The Wall Street J.*, Dec. 18, 2010. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052748704034804576025951767626460

[91] "What they know—Mobile," *The Wall Street J.*, Dec. 18, 2010. [Online]. Available: http://blogs.wsj.com/wtk-mobile/

[92] S. B. Wicker, "The loss of location privacy in the cellular age," *Commun. ACM*, vol. 55, no. 8, pp. 60–68, Aug. 2012.

[93] S. B. Wicker and D. E. Schrader, "Privacy-aware design principles for information networks," *Proc. IEEE*, vol. 99, no. 2, pp. 330–350, Feb. 2011.