Privacy Protection in Digital Rights Management Systems

by XiaoYu Chen , 9792470, University of Auckland

Abstract:

Digital Rights Managements (DRM) systems protect rights of all parties involved in digital content distribution. However, user privacy should not be neglected in DRM systems. This paper focuses on the privacy protection in Digital Rights Management systems. A detailed analysis of Fair Information Principle (FIP) that consists of some guidelines to help design a privacy-friendly DRM system will be carried out in this paper. And we will analyze the privacy protection mechanism in two different model DRM systems, one using digital battery and another using metadata strategy. We also analyze how they are compatible with the Fair Information Principle. Finally, we propose that we also need legitimate ways in privacy protection.

Digital content distribution is a quickly developing industry especially with the help of Internet. Some researchers even claim Internet-based market for digital content has a nice prospective future. At the same time, many Digital Rights Management systems are designed to help digital content providers to have some control over their digital content and obtain some usage information from users to some extent to let relative business entities make strategy decisions towards their market. However, user privacy should be also considered as “rights” of users. Such rights must be also protected in Digital Rights Management systems because the main goal of DRM systems is to protect rights of all parties involved in digital content distribution.

Of course personal information, such as home address, telephone number, credit card number, bank accounts, etc are definitely user privacy. Other people may consider age, disabilities, health records, etc as privacy, too. If such personal information is obtained by some non-relational parts, we can say that user privacy is jeopardized. And there might be even severe outcomes if malicious parts abuse such information. So DRM systems should have a good control over user information, if they collect and store such information not for malicious purposes. However, it’s not necessary that a DRM system should collect user information. But sometimes a DRM system may need to collect personal information of users if some digital service or digital content are provided to users for exchange. And many DRM systems need to collect some usage information about the utilization of their digital content. How to obtain such usage information while not damaging user privacy is an important open problem. A lot of web sites provide some kinds of digital content, such as freeware, shareware, or other kinds of digital content in order to gain feedbacks of evaluation, or just to increase the fame of their corporation for other business purposes, etc. Such web sites often require users to register before obtaining some digital content. Registration often needs to input some user information. Systems of these web sites managing digital content service can also be considered as primitive DRM systems. However, because users’ personal information is collected, user privacy may be jeopardized if such information is abused. If such corporations or web sites deliberately share or distribute users’ personal information with or to other parties without the permission of users, no technological solutions can help to solve this problem except by law. Now most corporations have various privacy policies that share the same goal, that is, to protect user privacy. We assume that they have good wills that they want users to know that they do want to protect user privacy, in addition to creating the so-called policies. So it is important for them to design a proper system to achieve this goal. We claim that if some common rules are obeyed in designing DRM systems, such systems will serve well both for corporations and users and all other parties.

The Fair Information Principle consists of several rules that are useful guidelines in properly designing a good DRM system serving all parties. A version of the Fair Information Principle consists of the following rules:

(1) Customizable Privacy

(2) Collection Limitation

(3) Database architecture and management

(4) Purpose Disclosure

(5) Choice

(6) Client side data aggregation and transferring processed data

(7) Competition of service

(8) Keeping business interests in mind

"Customizable Privacy" indicates that a DRM system should let system participants easily configure the system to accommodate their preferred information-collection and handling procedures. To some extent, the DRM system should provide system participants with choices for mechanisms of information collection and handling. System participants at least should include two kinds of people, administrators of the DRM system and users. Administrators can configure the DRM system to set up their preferred data-collection and handling mechanism. And users are also able to set up their preferred data-collection mechanism. The advantage is flexibility. Digital content providers can easily set the information collection mechanism background while providing some options to users. Just like P3P, a developing standard that lets users and providers negotiate about the information collection and handling mechanism before exchanging information. However, just like the conclusions stated in many research papers, it's easy to design such a protocol, but it's very hard to implement them. Or the cost of implementation is high. So most times we must simplify the problem. For example, if a user wants to register in a web site to obtain some digital content, he will be asked to provide some non-sensitive personal information during registration. Some information is mandatory, such as name and email address and gender. Some information is optional, such as physical address and telephone number. By "optional" it means the user can still register successfully without providing such optional information. Doing this provides some options for users. This is important because a system is not privacy-friendly if it requires a lot of personal information from users and stores such information. This rule also has another advantage compared with P3P. It is very easy to implement while P3P, is easy to design, very difficult to implement. And most times the cost of designing a DRM system should be reasonably low, the former is obviously a good choice for most business entities that provide some digital content.

The second rule of FIP, is Collection Limitation. A business entity should only collect information that it really needs and should disclose how this information will be used.

This prevents business entities from unlimitedly collecting user information and abusing such user information. However, we lack the accurate definition of “information that is really needed”. Some information that is not needed right now may be needed in the near future. For example, if a user wants to download a shareware, he may be asked to provide your email address, your name, physical address, etc. However, because it’s possible the user doesn’t buy the shareware after the evaluation period expires, user name and physical address should not be considered as necessary information. Alternatively, if the business entity wants to collect usage information, such as where the user is, it may ask the user to provide his country. That’s all. And if email address is collected, it should not be shared with a third party which may result in spam to the user. We claim that if some information is needed in the future, then such information must be collected in the future, now right now, through same or different channels. And staffs that are responsible for creating information collection policies should distinguish information needed right now from those that are not needed right now. Doing this will help protect user privacy.

The third is database architecture and management. If users’ personal information is stored in the database, it is particularly important to secure the database to protect privacy. It’s possible that several distributed databases store the same information. This redundancy has a catastrophic result: if security of one database is hacked, all other security methods provided in other databases are useless. So the entire privacy level of a distributed database system is the level of the weakest database. We recommend all distributed databases use the same security technologies and provide same extent in pseudonymization to keep consistency. And this will also make database management easy.

In DRM systems, Purpose Disclosure provides a way to communicate with users. So notices should be easily understandable and thoroughly distributed. It’s better to make notices tailored to different kinds of users. This can help users understand notices well. For example, providing notices in different languages is better than only providing English notices. However, this requires a DRM system knows the main language of users. And very few users consider providing their preferred language as “disclosing privacy”. This way can work well particularly for DRM systems involving a large set of users coming from a large set of regions or countries. Although this may create additional workload for the system, it is worth doing so because this can attract different kinds of users.

Choice in Fair Information Principle means a DRM system should give users reasonable choices for information collection. However, this is redundant to the first one in FIP to some extent. Both indicate some choices of data collection should be provided to users. But in the real live, a lot of companies want to collect more information than needed especially when they provide some digital service or digital content for exchange. They want such information for their own business purposes. And sometimes users must pay for using some digital content or digital service. So if a user pays by check, his name and mailing address may be disclosed to companies. And if he pays by credit card, his name and credit card number, which are absolutely his privacy, are collected by this company. Again, we need protection from companies. However, this guideline may be eliminated due to redundancy.

Client side data aggregation and transferring processed data put the task of privacy protection into users' computers. At least this puts part of the task of privacy protection into users' computers. This can be achieved with the help of some tools. Many users are concerned about their privacy. They use a lot of ways to protect their privacy. For example, they may use software which blocks cookies. They may use trusted proxy servers to achieve network anonymity. They may clean their hard disks from time to time in order to eliminate sensitive data. These can be achieved with the help of specific software which is considered as "privacy protection software" to some extent. And they even may provide bogus personal information when they are forced to provide personal information before accessing some digital content or obtaining some digital service from web sites that are not known to be trusted or untrusted. Providing personal information usually before registering in free email accounts or downloading some software are two examples.

The last two guidelines are business aspects. It is believed competition in the digital content provider and distribution market can result in better service to users. Because privacy is one of the users' demands, it should be improved by business entities which want to attract more users. Nearly all companies, web sites have a serious privacy policy is an example. One problem is that large business entities do have the technology and financial potential to do something in protection of user privacy. But some small business entities don't. They may converge with other business entities, so their policy may be subject to change from time to time. This may jeopardize user privacy due to very frequent change both in privacy policy and human resource. How to deal with monopoly is another problem. Monopoly eliminates competition. According to a research, 80% of music is controlled by only five business entities. These five business entities may ally and monopolize the relative distribution market. When they monopolize, users have no choice but to accept their possible unreasonable behaviors, including unfair privacy policies, if users still want to obtain such music. So at that time it's time for law to play a role. When designing a DRM system, we should also deeply understand the business operation and mechanism of the relative business entity. A lot of business investigations may be needed in advance. It's better that such a DRM system be designed internally by the business entity itself if it has good wills in user privacy protection.

The Fair Information Principle only consists of useful guidelines, not technological methods. So we can not force a business entity to implement such guidelines. And sometimes a DRM system doesn't need to be fully "compatible with" these guidelines. We can only suggest it to do so because it will do good to users, although this depends on the real will of the business entity. Incorporating such guidelines in a DRM system is not difficult. On the contrary, it will make low-cost and privacy-friendly DRM systems possible. The guidelines are subject to change from time to time to accommodate better guidelines.

Because a DRM system is itself a complicated software system, it have features of software systems. And now the "software system" manages user privacy. There may exist some trade-offs between excellent privacy and other system aspects, such as system performance, easy-to-use, resource use, cost, complexity of system management. It is possible such goals of software engineering can not be well achieved if we only consider providing better and better user privacy, neglecting such system aspects. In the real world, we need some negotiation among these aspects. A reasonable method is to have a DRM system incorporate some FIP features, not all. This is important for those small business entities because this will provide users with reasonable privacy protection while making the cost and other resource use at a tolerable level.

FIP is suitable for DRM systems that have a need to collect user information, especially when they need to collect some sensitive personal information. If a DRM system doesn't need to collect personal information and it can provide good control over the digital content, then the original goals of DRM systems have been achieved. Of course, user privacy is protected well. Clearly, the original goals of DRM systems are:

(1) Protect the rights of digital content providers. This is usually involving how to deal with the problem of unauthorized duplication of the digital contents. In other word, how to prevent piracy. The content provider needs some methods to control their digital contents after they are downloaded or sold. The control can fall into two aspects: making unauthorized duplication hard and making sure the legitimate user doesn't violate his access rights.

(2) Protect the rights of users. Users paid for the digital contents, and they obtain relative access rights which are provided by content providers. We claim that privacy protection is also a very important right of users. If some personal information is collected, then content providers are responsible for providing privacy protection to users. This can also be considered as a goal of DRM systems.

Follows are discussions of two sample DRM systems. We briefly discuss their mechanisms in digital rights management, and we also discuss the privacy protection mechanism in the two DRM systems.

Digital music is one of the most important and popular digital content worldwide. It involves a large number of people. It's easy to distribute and duplicate because tools have been commonplace among families. Together with software, digital music is also at the frontier against piracy. Many researches have been carried out to propose a good DRM system for digital music providers to protect rights of digital music providers and other relative entities, including authors and singers, etc. Of course user privacy should be considered in such DRM systems. However, the goals of the two DRM systems are the same.

(1) Make unauthorized copy (piracy) very difficult, thus protect rights of providers

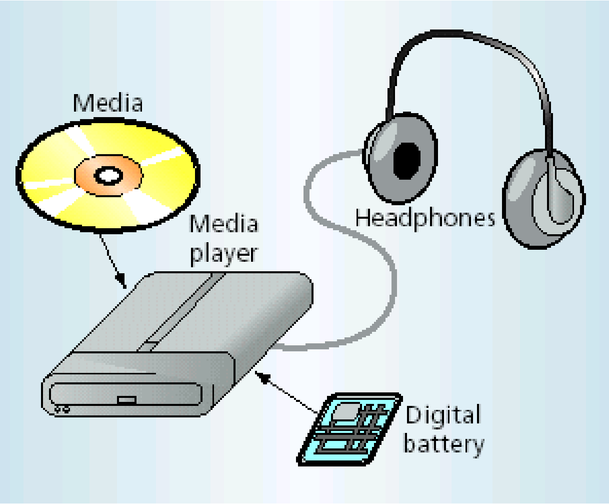
(2) Collect some usage information of digital music while not disclosing user privacy, thus provides useful business information to content providers and protects user privacy at the same time.

(3) The cost to implement such a DRM system should be reasonably low.

(4) The DRM system should remain transparent to users, or at least should not bring two much inconvenience to users.

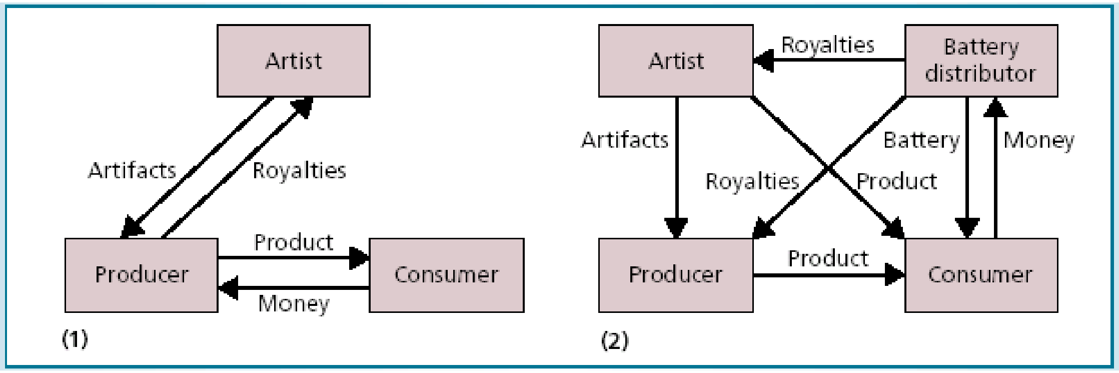
In these DRM systems, digital music providers need to collect some usage information of their music in order to develop their market strategy and distribute relative royalties to original authors or artists. Authors of more popular songs should get more royalties compared to authors of less popular ones. This is fair to authors. In other word, royalties should be based on their own “performance”. In the past, songs are recorded in CDs. Royalties are usually based on the number of CDs sold. However, because of the large piracy, music providers can not obtain accurate usage information only based on the number of CDs sold. We can see soon that with the DRM system model proposed by Tim Budd, it is possible to do this.

Tim Budd proposed a DRM system model based on per use. There is an invention, called “digital battery”, which is used in this DRM system. A digital battery is like a smart card which can store usage information. Digital batteries are installed into media players to provide power just like the usual batteries. The following picture demonstrates the use of digital batteries.



Quoted from reference [1]

In the past, authors and singers gave songs to producers, or called music providers. And users, or called consumers bought relative CDs from providers. Providers gave royalties to authors and singers based on the number of CDs sold. So there are three parties involved in music distribution, authors and singers, providers, and users. But now we have one more party, the battery distributors. Battery distributors can give royalties to providers and authors and singers based on the number of digital batteries sold and the usage information stored in digital batteries which are returned by users, just like the following pictures demonstrates:



Quoted from reference [1]

Digital batteries store usage information, such as which song is played and/or how many times it is played and/or the frequency it is played when users are using media players to enjoy music. After a period of time, users may run out of battery powers. They can return digital batteries to battery distributors and get a little refund. Battery distributors can extract usage information from those returned batteries and give such information to providers. Both providers and battery distributors can distribute royalties based on the usage information. Such a DRM system for digital music has the following advantages:

(1) If manufactured in large numbers in industry, a digital battery can be cheap. Just like a usual battery, it may last for several weeks or several months. Just like other daily items, any supermarkets, stores, can sell digital batteries. So it is easy to acquire a digital battery. Because it functions just like a battery, it’s easy to use. Its limited lifetime guarantees that users must buy new digital batteries from time to time. This is where the royalties come from. Users may also recharge their digital batteries in designated places after reasonable payment.

(2) The usage information stored in digital batteries can provide statistic information about given music. Users are encouraged to return their digital batteries that are out of power to get a little refund. Even some users don’t return their used digital batteries, providers have more revenue because no refunds are needed. Due to some refunds if digital batteries are returned to battery distributors, we can claim that the number of users who are not willing to return their used batteries must be low because there is definitely no harm in returning digital batteries, but financial interests can be gained. And users can recharge their digital batteries in some designated stores. A recharging machine first reads usage information stored in batteries, then sweeps such information and recharges batteries. This may also involve a reasonable payment for recharging. And usage information is obtained. Such stores can transmit such usage information in a large bundle to music providers.

(3) Users need to buy digital batteries to have their media players function properly. There is no need to provide personal information when buying digital batteries. There is also no need to provide personal information when returning digital batteries or recharging batteries. Such work can be done in any designated stores or markets. We have stated that digital batteries only store usage information. So user privacy is excellently protected. No personal information is disclosed.

(4) There can exist many kinds of digital batteries which are all compatible with each other and media players. Quality difference may exist. So there will be great competitions in the market of digital batteries although manufacturers must have license to manufacture digital batteries. Such business competition can do good to users.

(5) With the technology of smart card, digital batteries face the same attack problem. However, the problem can not be harder than that appears in smart card. The same technology can be used in building digital batteries along with some methods of cryptograph. So no new technology is needed. This can make the cost of manufacturing digital batteries low and it is also easy to be accepted by business

entities because adopting new technologies often involves a high cost. If a solution is easy to be accepted by users and refused by business entities, it is not a good solution, either.

(6) The same DRM system can apply to other digital content, such as pictures, electronic books and magazines, copyright digital files, etc.

(7) Digital batteries remain transparent to users. They don't put a burden onto users. So they are easy to be accepted by users, too. Because media players are developing quickly, we can claim that in the near future, they can incorporate digital batteries which may become a standard. So digital batteries do provide a prospective solution to digital music in the field of anti-piracy, privacy protection and business development.

Now we take a look at the digital battery solution to check how it binds with the Fair Information Principle. For customizable privacy, this can be set in digital batteries. For example, providers can set batteries to collect information about how often a song is played, how many songs are played in a designated period of time, what songs are played, etc. This may involve micro-programming in chips of digital batteries. Of course more memory is needed in digital battery if more information is collected. This is still transparent to users. So many choices of information collection mechanism are available. So here providers can easily set the information collection method while not damaging user privacy. For collection limitation, it is excellently achieved in digital battery solution because only usage information that is really needed by content providers is collected. Databases of content providers now need only to store such usage information, no user personal information. And disclosures can be accompanied by the selling of digital batteries. It's convenient to do this. Digital battery solution also provides an excellent client-side data aggregation. According to the FIP, only such aggregated data is collected (transferred) by providers. As far as the competition of service is concerned, we have mentioned that there may be many digital battery producers that compete with each other. So we can claim that the digital battery solution is an excellent DRM system model that is fully compatible with the FIP principle.

Digital battery solution will face the same problem in smart card. That is fraudulent use attacks. Other problems may also occur. For example, digital battery requires all media players only use digital batteries. No other kinds of batteries are needed. This requires changes in hardware devices to be compatible with digital batteries. Currently the solution is not a standard yet. However, because this paper mainly focuses on the privacy protection in DRM systems, detailed discussions of other aspects of the DRM system are beyond the scope of this paper. Buy we can not neglect one important disadvantage in the digital battery solution. It does not support digital content distribution via Internet. Or user computers can not play such digital content that can only be played in devices installing digital batteries. It's because if user computers can play such digital content, the digital battery solution will fail. In other word, Internet, which is a rather quickly developing technology, having more and more impact on everything in our lives, can not play a role in the DRM systems using digital batteries. Follows we propose an alternative DRM system model which utilizes Internet. We focuses on the downloaded music. How to prevent piracy will be briefly discussed and how to protect user privacy will also be discussed in detail. We don't discuss digital content recorded in CDs because this mainly involves anti-piracy problem, not privacy protection. And the anti-piracy, which is an open problem, remains not completely solved yet.

Internet has made information exchange quick and convenient. However, because users can also freely exchange digital content via Internet, anti-piracy, which involves how to prevent unauthorized copies, is an open problem for research. Most users have experience downloading some digital content. Now we want a simple DRM system which manages downloaded digital music well and provides reasonable privacy protection at the same time to users.

We use the metadata strategy. We can consider metadata as some digital information that describes the rights owned by relative users. These rights are specified by music providers. One advantage of metadata is that such data is tied with digital content, not user computers or users themselves. And an application is also needed to manipulate the metadata. Metadata is persistent with digital content. The application can modify the metadata so that user rights can be manipulated in a specified way. For example, digital music files are very commonplace in Internet. One of the most popular kinds of digital music files is MP3 file. A MP3 file also encodes some extra information at the head of the file. Such information may include the names of the singers, music providers, and authors. We can claim that MP3 have become a de-facto standard in digital music format due to its compact size of files and high quality in playing. However, digital format is developing quickly. More and more formats are expected to appear in the near future. And some de-facto standards which are welcomed by all may also appear. It's not difficult to encode some metadata in such a format. And media players running in user computers can be the applications to manipulate such metadata. Of course we need proper media players from relative providers. We just claim that with the fast developing IT industry, it's not difficult to achieve a new standard including new digital music format with proper encoding mechanism and the new media players. When a user wants to run a media player to play a music file, the player may first check the metadata in the music file to see whether the user has permission to play it. Or, in other word, if rights specified by the encoded metadata are violated if the file is played, the media player refuses to play the file. If the file can be played without violating the rights specified by the relative metadata, the media player first modifies the metadata if necessary and then plays the file. Many rights can be specified by metadata, such as times to play, date to expire, etc. For example, a file can not be played after its expiry date. So the media player needs to compare current date with the expiry date encoded in metadata. For the problem that a file can only be played for a limited number of times, the metadata needs to store the current times played. And the media player needs to modify (plus 1) the encoding metadata before and after one-time play. There are also other special rights, such as frequency (the maximum number a file can be played in a day or week, for example). In one word, metadata can encode many rights. And users even can update the rights. In other word, "rights" can also be downloaded from without. Users can play files according to the rights specified by the metadata encoded. And media players can communicate with providers with the usage information via Internet. It's usual that users make some payment and/or registering in relative web sites before downloading files or "rights". Here user privacy is affected to some extent. In additional to information provided to web sites, user's IP address is disclosed to web sites due to the FTP or HTTP protocol. Can IP address be considered as user privacy? Different people may have different opinions. If the IP address is dynamically allocated and belongs to a large ISP which has a large number of IP addresses to allocate, disclosing an IP address for a small period of time may not be considered as disclosing privacy because the IP address will be reclaimed by the ISP after a while. Most dial up (modem) users belong to this situation. However, more and more people are using cable modems to connect to Internet. Their IP addresses are static, disclosing such static IP addresses may result in severe security problems, such as hacking and incoming virus and trojans. Serious and conscious cable Modem users may recognize such problems. They may use anti-virus programs and firewalls to minimize potential security risks. Also they can use trusted proxies to hide their IP addresses. So how to distinguish trusted proxies from those untrusted ones is also a problem. Usually trusted proxies belong to large network companies which are very concerned about security, including user privacy. Users may obtain better proxy service if they pay for proxy use, as registered users, such as the mechanism of www.anonymizer.com. However, large network companies might also be large and attractive targets for hackers. So the security mechanisms as well as privacy protection in such companies are important to users. And it is also important for users to select a good company. Some ISPs also mark users' IP addresses to enhance privacy. The servers of ISP may also function as proxies for users to filter malicious codes, etc. And sometimes for a company user, he may also need to hide his IP address for privacy reasons. The same technologies may apply to help. For the metadata strategy, users can update the rights from specific web sites. This will also involve downloading operations. We can claim that with the protection technologies mentioned above, most users can effectively protect their privacy if they really want to do so. Here for the metadata strategy DRM system, we neglect some small problems that may appear under some special situations. For example, a user may not have write permission in an operating system, so the media player (metadata manipulation program) can not make modifications in metadata.

Again we want to look whether the metadata solution is "compatible" with the FIP principle. It depends on the providers to create the policy for collecting information, as mentioned above. And it also depends on the providers' wills to collect the kinds of user information. Because usage information is transferred by the media players via Internet and such operations may be transparent to users, it's very important to design "honest" media players that only transfer real usage data. There may be some trusted agencies that design such media players. In other word, users gain digital music and media player from different entities. However, as we have seen, the metadata solution described above doesn't incorporate FIP well enough compared with the digital battery solution.

It's also worth the time to mention the security methods which can be used in metadata strategy DRM systems although they are not related to user privacy. With this kind of DRM system, the metadata is the target for hacking. The obvious operation is the attempt to "fabricate" "bogus" metadata in files to "gain" additional rights. So some encryption methods may be used to protect metadata. For example, users may obtain unique keys from content providers. The relative application (media player) can use the keys to make decryptions. Another hacking operation is to modify the codes of manipulation programs to let them "bypass" the "metadata-checking" routine. So software obfuscation technique must be used in such applications.

The last part of this paper is to raise an opinion. Technologies are not all we need to protect user privacy. Only companies and users with good wills can effectively protect user privacy using such technologies because privacy protection needs real activities among all parties. A malicious party can deliberately jeopardize user privacy. For example, cheaters may create bogus e-commerce web sites that attract innocent customers. If customers disclose personal information to these sites, for example, if their credit card numbers and names are known to such a malicious party, very severe outcomes may occur. Such activities are network crimes which need more co-operations among various companies, departments, and countries. We also need laws to protect user privacy because there are many companies that don't want to really protect user privacy. So users can only refer to laws for help. There are already some privacy laws in United States and Europe. But many other countries lack such laws. In addition to laws, we also need co-operations as mentioned above.

Different DRM systems may have different operating mechanisms and different methods in privacy protection. However, privacy protection is an important aspect that cannot be neglected in DRM systems. And with the development in markets of digital content distribution, more and more business entities will realize that their success will largely depend on good DRM systems with good privacy protections that make users safe.

Reference:

[1] T Budd, "Protecting and Managing Electronic Content with a Digital Battery", IEEE Computer, 2-8, August 2001.

[2] J Feigenbaum, M Freedman, T Sander, A Shostack, "Privacy Engineering for Digital Rights Management Systems". In Workshop on Security and Privacy in Digital Rights Management 2001.

[3] S Bechtold, "From Copyright to Information Law – Implications of Digital Rights Management". In Workshop on Security and Privacy in Digital Rights Management 2001

[4] Alexander Rossnagel, Rudiger Grimm, "Can P3P Help to Protect Privacy Worldwide?" ACM Multimedia Workshop 2000

[5] R Merkle, "Protected Shareware: A Solution to the Software Distribution Problem." dated "October 19, 1998" and marked ", Copyright 1993 by Xerox Corporation".

[6] Valimaki, M.; Pitkanen, O. ," Digital rights management on open and semi-open networks", Internet Applications, 2001. WIAPP 2001. Proceedings. The Second IEEE Workshop on , 2001

[7] Hartung, F., Ramme, F., "Digital rights management and watermarking of multimedia content for m-commerce applications", IEEE Communications Magazine , Volume: 38 Issue: 11 , Nov. 2000

[8] Edward J. Grenier, "Computers and privacy", Proceedings of the ACM symposium on Problems in the optimization of data communications systems October 1969

[9] David M. Kristol, "HTTP Cookies", ACM Transactions on Internet Technology (TOIT) November 2001, Volume 1 Issue 2

[10] Jason Catlett, "Open letter to P3P developers & replies", Proceedings of the tenth conference on Computers, freedom and privacy.

[11] Kenneth C. Laudon, "Markets and privacy", Communications of the ACM September 1996, Volume 39 Issue 9