Privacy issues with DRM

Jalaj Pandey

*This post has been written by Jalaj Pandey interning at CIS. It elaborates upon the various privacy issues with the Digital Rights Management. The author talks about the various ways in which content producers use DRM as a tool to infringe the privacy of the end users.*

The ubiquity of internet in today’s world has made content and information sharing an easy task.[[1]](#footnote-1) A certain media file can be shared and made public with hardly any technical obstacles.[[2]](#footnote-2) Issues like hacking, unauthorized copying and publication, unlicensed usage have become concerns for content producers, who have employed Digital Rights Management (hereafter DRM) measures to address some of them.

Several instances of the online privacy intrusion by the content producers have been recorded.[[3]](#footnote-3) In such a scenario the balancing the rights of the content producers and the end users becomes an important one. It is imperative to find a common ground to safeguard the interests of both the parties involved. In the recent past DRM has been receiving a lot of flak[[4]](#footnote-4) because of the privacy issues contented by the users.[[5]](#footnote-5)

In the most rudimentary form privacy can be explained as any information about an individual which he/she does not want to be made public. It is important to mention that this information is seen from the perspective of an ordinary reasonable person. The UN Declaration of Human Rights, 1948, defines privacy as a fundamental right of every human.[[6]](#footnote-6) The functioning of the DRM is based on restricting the usage or distribution of the content. Since this restriction is only possible after there is a formal identification of the end user,[[7]](#footnote-7) the content producers end up collecting information about the users. For example: a DRM for a music file might work in a manner where it can only be accessed by one computer from which the user accesses and registers for the first time.[[8]](#footnote-8) DRMs initially identify the IP addresses of the system and make the file functioning on only that IP address.[[9]](#footnote-9) In this way the producer ends up collecting information about the end user. Different DRM models take different ways to collect information of their user.[[10]](#footnote-10) While collecting IP addresses[[11]](#footnote-11) in one of them the other way is tracking the user information via download,[[12]](#footnote-12) browsing activities, subscription service,[[13]](#footnote-13) etc. The usage log of the users is generated and becomes a valuable asset to assess and predict the preferences of the users

Two contentions of privacy have been raised on the privacy issues of DRM -

1. What is the accountability of this process and
2. Whether it puts the content producers in a position where they can control the users.

The information collected is under the control of content producers, who mostly store this information in the form database. BEUC (European Consumer Organization) claimed that the DRM systems technologically enable content providers to monitor private consumption of content, create reports of consumption, and profile users.[[14]](#footnote-14)

The information is at the disposal of the content producers. An assessment of DRM applications under Canadian Privacy showed that the firms did not even recognise privacy issues of the customers as a priority.[[15]](#footnote-15) In fact the firms failed to provide the information that was stored in their databases.[[16]](#footnote-16) This gives an idea about the lack of transparency that exists in collecting the information about users. The question whether users are aware of what information is being collected and to what extent they are being tracked online remains unanswered. The CEN/ISSS (European Committee for Standardization/ Information Society Standardisation System) pointed out that DRMs have a large potential to transmit, generate personal information about users.[[17]](#footnote-17) It has also been characterized by unprecedented levels of monitoring by various content producers.[[18]](#footnote-18)

Further the principled level argumentation to this is on lines of collection of information without any authentication from the user herself/himself. It is essential that if any information is collected or saved by the producers it should only be after taking consent of the user.[[19]](#footnote-19) Surveillance and compelled disclosure of information about intellectual consumption threaten rights to personal integrity.[[20]](#footnote-20)

DRMs take away the anonymity of the consumption.[[21]](#footnote-21) Since the producers can practically monitor the content usage of the user, this has led to wide scale of price discrimination.[[22]](#footnote-22) This means that producers would monitor and assess the preferences[[23]](#footnote-23) of the user and subsequently raise the prices of that particular class of products.[[24]](#footnote-24) In the report of FIPR (Foundation of Information Policy and Research) it was found that Microsoft had been trying to implement their DRM systems in their products using a similar approach to gain a monopoly position as in their strategy of browser implementation.[[25]](#footnote-25)

The **Sony BMG copy protection rootkit scandal[[26]](#footnote-26)** in 2005 brought much criticism to DRM. It was found out that Sony BMG had introduced illegal and harmful copy protection measure in its CDs. The rootkit element of the software is used to hide virtually all traces of the copy protection software's presence on a PC, so that an ordinary computer user would have no way to find it. Further more than just the DRM part of it the software also made the user’s system open to a number of malwares and created vulnerabilities in the system. Sony was eventually made to compensate consumer costs, etc on the same. However the question of whether the database in the hands of companies can be used in arbitrary manner was intensely discussed after this.[[27]](#footnote-27)

It is essential that an effective framework is brought into effect which caters to privacy interests of the users. Privacy is the basic human right and it is the onus of the State to protect and safeguard this right. It is essential that the State does not compromise and support mechanisms which promote the welfare of the content producers over the users. The balance of users and producers becomes all the more important in a developing country like ours. The lack the awareness and the knowledge coupled with increasing usage of internet can lead to the exploitation of many. It is essential that the States see through these problems and collectively find an all encompassing solution to it.

1. K. G. Coffman and A. M. Odlyzko, Growth of the Internet, AT&T Labs – Research, July 6, 2001, available at, ([www.dtc.umn.edu/~odlyzko//doc/oft.internet.growth.pdf](http://www.dtc.umn.edu/~odlyzko//doc/oft.internet.growth.pdf)) (hereinafter Growth). [↑](#footnote-ref-1)
2. The Daily Source, The Growing Impact of the Internet, April 4, 2016, available at (https://www.dailysource.org/about/impact). [↑](#footnote-ref-2)
3. Corryne Mcsherry, Adobe Spyware Reveals (Again) The Price Of DRM: Your Privacy And Security, Electronic Frontier Foundation, October 17, 2014, available at,

   (https://www.eff.org/deeplinks/2014/10/adobe-spyware-reveals-again-price-drm-your-privacy-and-security). [↑](#footnote-ref-3)
4. Digital Rights Management: A failure in the developed world, a danger to the developing world, Electronic Frontier Foundation, March 23, 2005, available at,

   (https://www.eff.org/wp/digital-rights-management-failure-developed-world-danger-developing-world). [↑](#footnote-ref-4)
5. R. Subramanya and Byung k. Yi, Digital Rights Management, available at, (<https://www.academia.edu/8054608/Digital_Rights_Management>) (hereinafter Digital Rights Management). [↑](#footnote-ref-5)
6. Global internet liberty campaign, privacy and human rights, An International Survey of Privacy Laws and Practice, available at, (http://gilc.org/privacy/survey/intro.html). [↑](#footnote-ref-6)
7. Ann Cavoukian, Privacy and Digital Rights Management (DRM): An Oxymoron, Information and Privacy Commissioner Ontario, available at, (https://www.ipc.on.ca/images/Resources/up-1**drm**.pdf ) (hereinafter Oxymoron) [↑](#footnote-ref-7)
8. Varian, H.R. (1985) ‘Price discrimination and social welfare’, American Economic Review, Vol. 75, available at, (http://www.economics-ejournal.org/economics/journalarticles/2007-1/references/Varian1985). [↑](#footnote-ref-8)
9. Privacy and Digital Rights Management,A position paper for the W3C workshop on Digital Rights Management, January 2001, available at, (www.w3.org/2000/12/drm-ws/pp/hp-poorvi.html). [↑](#footnote-ref-9)
10. Growth supra note, 1. [↑](#footnote-ref-10)
11. Digital Rights Management supra note, 5. [↑](#footnote-ref-11)
12. Thierry Rayna, Privacy or piracy, why choose? Two solutions to the issues of digital rights management and the protection of personal information, Intellectual Property Management, Vol. X, No. Y, available at,

    (www.inderscienceonline.com/doi/abs/10.1504/IJIPM.2008.021138). [↑](#footnote-ref-12)
13. Oxymoron supra note, 7. [↑](#footnote-ref-13)
14. BEUC, Consumentenbond, and CLCV at DRM Working Group 1 (2002), available at, (https://privacy.org.nz/assets/Files/4558510.pdf). [↑](#footnote-ref-14)
15. Natali Helberger and Kristo´f Ker´enyi and Bettina Krings, Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations, available at (citeseerx.ist.psu.edu/showciting?cid=733532). [↑](#footnote-ref-15)
16. Knud Bohle, Indicare, Research into unfriendly DRM : A Review, December, 2004,available at, (citeseerx.ist.psu.edu/showciting?cid=733532) (hereinafter Indicare). [↑](#footnote-ref-16)
17. European Committee for Standardization/Information Society Standardisation System (CEN/ISSS) DRM Report, 2003. [↑](#footnote-ref-17)
18. Indicare supra note, 16. [↑](#footnote-ref-18)
19. News Release, “Forrester Technographics Finds Online Consumers Fearful of Privacy Violations” (October 27, 1999 available at, (www.forrester.com/ER/Press/Release/0,1769,177,FF.html). [↑](#footnote-ref-19)
20. Julia E. Cohen, Georgetown Law Faculty Publications, DRM and Privacy, January 2010, available at,

    (https://www.academia.edu/2164013/DRM\_and\_Privacy). [↑](#footnote-ref-20)
21. Thierry Rayna, Privacy or piracy, why choose? Two solutions to the issues of digital rights management and the protection of personal information, Intellectual Property Management, available at, ([www.inderscienceonline.com/doi/abs/10.1504/IJIPM.2008.021138](http://www.inderscienceonline.com/doi/abs/10.1504/IJIPM.2008.021138)) (hereinafter Privacy or piracy). [↑](#footnote-ref-21)
22. Moe, W. and Fader, P. (2004) ‘Dynamic conversion behavior at e-commerce sites’, Management Science, Vol. 50, available at,

    (https://www.researchgate.net/publication/227447618\_Dynamic\_Conversion\_Behavior\_at\_E-Commerce\_Sites). [↑](#footnote-ref-22)
23. Privacy or piracy supra note, 21. [↑](#footnote-ref-23)
24. Sismeiro, C. and Bucklin, R. (2004) ‘Modeling purchase behavior at an e-commerce web site: a task completion approach’, Journal of Marketing Research, available at, (citeseerx.ist.psu.edu/showciting?cid=906878). [↑](#footnote-ref-24)
25. Ross Anderson, Foundation of Information Policy and Research Consultation Response to DRM (2004), available at, (www.**fipr**.org/APIG\_**DRM**\_submission.pdf). [↑](#footnote-ref-25)
26. Otto Helweg, Sony, Rootkits and Digital Rights Management Gone Too Far, Oct, Oct. 31, 2014, available at (https://blogs.technet.microsoft.com/markrussinovich/2005/10/31). [↑](#footnote-ref-26)
27. Sony BMG Litigation Info, Electronic Frontier Foundation, available at, (https://www.eff.org/cases/sony-bmg-litigation-info). [↑](#footnote-ref-27)