

디지털 저작권과 프라이버시의 경합과 균형

이 남 용*

요 약

이 글의 목적은 디지털 저작권과 프라이버시 사이의 경합적 요인을 분석하고 균형을 위한 대안을 제시하는데 있다. 현재 대부분의 디지털 저작권 보호기술의 핵심은 사용자를 식별할 수 있는 방법에 있는데, 이러한 사용자 식별은 익명성을 기반으로 하는 프라이버시에 대한 침해요인이 되고 있다. 이와 같은 경합적 요인을 해결하기 위해 익명성을 보장하는 디지털 저작권 관리기술들이 많이 제안되었으나, 그 대부분이 부분적인 문제에 대한 프로토콜의 형태로 이루어진 대안으로, 현재의 인터넷 환경, 사용자의 행동양식, 경제적 요인 등과 부합하지 않는 측면이 많아 적용하기 곤란하다. 한편, 디지털 저작권 보호를 위한 여러 기술적 노력들도 사실상 저작권 보호 효과는 미미한 반면, 사용자의 권리와 프라이버시에 대한 침해요인을 증대시키고 있다. 현재의 상황은 디지털 저작권과 프라이버시의 균형을 위한 기술적 해결이 요원한 상태이다. 이러한 상황에서 균형을 위한 대안으로 법률에 의한 조정과 새로운 비즈니스 모델을 통한 디지털 저작권 보호가 효과적임을 주장하고자 한다. 즉, 기술적 완벽성보다는 사용자 편리성에 의한 실질적인 저작권보호와 법률과 사용자 계도를 통한 프라이버시 보호를 제안한다.

1. 서 론

디지털 정보의 일상화, 컴퓨터 네트워크의 확대 등과 관련된 기술의 발전은 정보이용 및 분배에 있어서 신속성과 편리함을 제공하지만, 동시에 개인 프라이버시 침해문제를 야기하고 있다. 많은 인터넷 사용자의 개인 정보는 사용자의 부주의 또는 서비스제공자(예, ISP, 웹사이트)의 잘못된 의도에 의해 유출되어 프라이버시 침해요인이 되고 있다. 이에 대해 인터넷 이용에서의 프라이버시 보호를 위한 기술적 연구와 법률개정에 대한 요구가 증대하고 있다.

앞서 거론한 인터넷 관련 기술의 발전은 인터넷 사용자에 대한 프라이버시 침해와 함께 디지털 저작권침해의 문제도 야기하였다. 디지털 정보는 관리와 이동이 간편하다는 점, 복사본과 원본의 차이가 없고 복사가 편리하다는 점, 그리고 인터넷을 통한 다자간 공유가 용이하다는 점 등에 의해 불법복제가 광범위하게 진행되고 있으며, 이로 인해 지적재산권이 심각하게 침해받고 있는 실정이다. 이러한 문제를 해결하기 위해 디지털 지적 재산권보호에 관한 법률(예, 미국의 DMCA - Digital Mille-

num Copyright Act⁽¹⁾)이 제정되는 한편, DRM (Digital Rights Management)이라는 디지털 저작권 관리기술이 제안되었다.

DRM의 핵심은 암호, 데이터 은닉 등 여러 요소기술들을 종합적으로 사용하여 저작권보호를 필요로 하는 디지털 콘텐츠의 사용규칙을 사용자에게 강요하는데 있다. 그러나, 사용자에게 콘텐츠에 대한 사용규칙을 강요하는 과정에서 사용자의 정당한 권리와 프라이버시가 침해받을 가능성이 높다^(2,3,4). 또한, 기술적인 측면에서 보면 DRM의 가장 핵심적인 부분은 사용자의 식별(Identification)인데, 이는 프라이버시보호의 가장 중요한 요소인 익명성(Anonymity)에 직접적인 위협이 된다. 즉, 디지털 저작권과 프라이버시는 서로 경합하는 가치가 되었다⁽³⁾.

프라이버시라는 개념이 생긴 이래, 프라이버시는 절대적 기본권이라기보다는 다른 사회적 가치(예, 공공의 이익)와 비교 경합되어 시대 또는 사건에 따라 상대적으로 평가되어왔다. 이와 같은 의미에서 지식정보화 사회에서의 프라이버시, 특히 디지털 콘텐츠의 이용과정에서 침해받을 우려가 있는 프라이버시의 상대적 가치를 알아보는 방편으로 디지털 저작권과 비교 평가하고자 한다.

* 인제대학교 컴퓨터응용과학부 기초과학연구소 (nylee@inje.ac.kr)

이 글의 목적은 디지털 저작권과 프라이버시 사이의 경합적 요인을 분석하고 균형을 위한 대안을 제시하는데 있다. 이 글에서 다루고자 하는 내용과 유사한 선행연구(프라이버시와 여타 가치들과의 충돌문제)들은 대부분 서로 대립되는 양 가치 중 어느 하나를 일반적으로 지지하는 양극화를 지향하고 있다. 비록, 균형을 도모하는 방안을 제시하려는 노력은 있으나, 연구자의 기본적인 이념적 성향을 크게 벗어나지 못하고 있다.^{2,3,4,5,6,7,8,9}. 이러한 현상은 이 글에서도 크게 다르지 않게 나타날 것이다. 이는 가치판단의 기준이 개인에 따라 다를 수밖에 없다는 측면에서 당연한 결과이다.

이 글에서 제시하는 문제점 분석이나 대안들은 기술발전과 경제적 요인에 대한 저자의 주관적 예측에 기초하였음을 밝히고자 한다. 이 글에서 거론하고자 하는 디지털 저작권과 프라이버시 문제는 모두 인터넷 관련 기술의 발전에 기인하고 있으며, 이러한 기술에 대한 고려가 없는 대안은 한계가 있을 수밖에 없다. 프라이버시를 열렬히 옹호하는 모임 cyberpunk⁵는 “법이 아닌 기술에 의한 프라이버시 보호”를 주장하고 있다. 그러나, 이러한 목적으로 제시된 프라이버시를 향상 시키는 기술(PET - Privacy Enhancing Technologies)의 대부분은 기술적인 문제 또는 경제적이고 관습적인 이유에 의해 현재 적용하기 곤란하다. 한편, 아날로그 시대의 저작권과 동일한 것을 디지털 저작권에서 요구하는 것도 문제가 있다. 새로운 환경에 적합한 새로운 저작권 개념과 함께 새로운 비즈니스 모델이 요구된다.

기술적 해결의 가능성이 요원한 상태에서 취할 수 있는 방안으로 “악용가능성을 최소화한 법에 의한 조정”과 “디지털 콘텐츠를 위한 새로운 비즈니스 모델을 통한 실질적인 저작권 보호”를 제시하고자 한다. 미국의 DMCA는 디지털 저작권보호의 본래 목적과는 다르게 악용된 사례가 많은데 이는 디지털 저작권 침해행위 자체를 기술적인 측면에서 파악하기 힘들다는데 기인하고 있다.¹¹. 그러므로, 디지털 저작권 보호 관련 법률을 제정하기 위해서는 법률 집행에 필요한 기술의 한계를 명확히 인식해야 한다. 한편, 새로운 비즈니스 모델은 진화해 가는 인터넷 환경에 맞추어 서서히 등장할 것으로 예상된다. 이러한 변화를 유도하는 기본적인 요소는 디지털 저작권의 경우 경제적인 요인이 될 것이다. 한편, 프라이버시 보호기술을 촉발시키는 시장형성이 불안정한 현재로서는 법률에 의한 유도가 요구된다.

이 글은 다음과 같이 구성되어 있다. 2 장에서는 DRM 기술의 핵심이 되는 식별을 중심으로 이에 따른 프라이버시 침해 가능성을 살펴보고자 한다. 3 장에서는

PET 기술의 현황과 그 문제점을 살펴보고, 4 장에서는 디지털 저작권과 프라이버시의 균형을 위한 대안을 제시하고자 한다. 5 장에서 이 글에 대한 결론을 다루고자 한다.

II. DRM 기술

이 장에서는 복제방지, 이용권한에 따른 접근제어, 크래킹방지, 정보오닉, 모호화(obfuscation), 불법사용추적 등의 DRM의 요소 기술에 대해 살펴보고자 한다. 특히, 사용자의 프라이버시의 핵심에 해당하는 익명성(Anonymity)에 대한 DRM의 영향을 중점적으로 다루고자 한다.

디지털 저작권과 관련하여 주목해야할 디지털 정보의 주요 특징을 살펴보면 다음과 같다.

- (D1) 완벽하고 간편한 복제
- (D2) 컴퓨터 네트워크를 이용한 빠른 확산
- (D3) 다수의 사용자간의 공유

특징 D1은 디지털 정보의 본연적 것인 반면, 특징 D2와 D3은 1990년대 후반 인터넷 사용자의 급격한 증가와 여러 데이터 압축 및 네트워크 기술의 발전에 기인하고 있다. 특히, 특징 D2는 CD-RW등에 의한 물리적 복제가 가질 수밖에 없는 시간지연의 문제를 해결한 것이고, 특징 D3은 불법 복제된 콘텐츠에 대한 대규모 데이터베이스의 존재 가능성을 의미한다. 특징 D2와 D3은 P2P (Peer-to-Peer) 파일공유(예, Napster, 소리바다)가 디지털 저작권 침해에 큰 역할을 했다는 측면에서 중요한 특징이다.

DRM의 주요 방법의 하나는 암호를 이용한 접근제어이다. 즉, 사용자에게 제공되는 디지털 콘텐츠는 암호화된 형태로 제공된다.

$$E_k(m), ID_m$$

여기서, E 는 암호함수를 ID_m 은 디지털 콘텐츠 m 에 대한 식별자로 사용자가 비밀키 k 를 요청할 때 이용된다. 비밀키 k 와 콘텐츠 m 에 대한 사용규칙 L_m 을 사용자에게 인지하지 못하게 분배하는 방법이 대부분의 DRM 시스템에서 가장 핵심적인 부분이다. 이를 위해 주로 사용하는 방법은 역시 암호를 이용하는 것으로 다음과 같은 형태로 비밀키와 사용규칙이 사용자에게 제공된다.

$$E_{UL}(k, L_m)$$

여기서, UI(User Identifier)는 사용자를 식별하기 위한 정보로 사용자가 인지하거나 또는 타인에게 양도하기 어려운 정보를 주로 이용한다.

이 방법의 문제는 사용자를 식별할 수 있는 정보 UI가 DRM 서비스를 제공하는 타인에게 제공되어야 한다는 점이다. 이는 프라이버시 보호의 가장 중요한 요소의 하나인 익명성(Anonymity)이 더 이상 보장되지 않음을 의미한다. 프라이버시를 향상시키는 DRM에 대한 많은 기술적 제안들은 이 부분에 집중되어있다^(10,11).

불법 사용자를 사후 추적하거나 사용을 차단하는 형태의 저작권 보호 방법도 있다. 이때 주로 사용하는 방법은 데이터 은닉인데, 이는 콘텐츠 자체에 시청각적으로 감지하기 어렵고 제거 불가능한 형태로 인식정보를 삽입하여 사후 추적이나 복제방지에 이용하는 방법이다. 데이터 은닉기술이 디지털 콘텐츠 저작권보호의 방법으로 주목받게 된 가장 큰 이유는 암호를 이용한 콘텐츠 접근제어는 콘텐츠의 특성상 암호가 해제된 상태로 소비되어야 하며, 그러한 상태에서의 불법복제는 암호로는 도저히 막을 수 없다는 사실에 있다. 이러한 이유로 데이터 은닉은 1990년대 말 워터마킹이라는 기술로 상당한 가능성을 보이는 듯 하였으나, 정당한 사용자도 데이터 은닉과정에서 발생하는 콘텐츠의 열화를 감수해야 하고 기술적으로 구현이 어렵다는 문제가 있어 현재는 그 가능성에 대한 기대가 현격히 줄어든 상태이다. 이러한 현상은 워터마킹을 이용하여 디지털 음악의 저작권보호를 위해 결성된 모임 SDMI가 실패한 후에 더욱 두드러지게 되었다⁽¹²⁾.

DRM은 Microsoft, InterTrust, Adobe, IBM 등 여러 기업에서 활발히 그 개발이 진행되고 있으며, 현재 일반 PC는 물론, mp3 플레이어, 핸드폰 등에도 적용되고 있다. 그러나, 기존의 DRM은 저작권 보호에 사용자의 프라이버시 보호가 직접적으로 필요하지 않다는 이유로 이를 중요하게 다루지 않고 있다. 이로 인해 현재의 DRM 기술에서는 저작권 관리에 있어서 사용자 인증 또는 콘텐츠의 불법사용 감시를 위한 사용내역 보고과정에서 사용자의 프라이버시(사용자의 구매내역 및 취향)가 침해될 가능성이 높다.

DRM의 프라이버시 침해가능성에 대한 우려는 많은 연구자에 의해 지적되었다^(2,7,8). 그러한 우려 중에서 가장 큰 주목을 받았던 내용들은 UI의 유출에 의한 프라이버시 침해가능성과 함께, Microsoft의 DRM OS⁽¹³⁾와 Intel, IBM, HP, Microsot를 중심으로 한 TCPA(Trusted Computing Platform Alliance)⁽¹⁴⁾에 의해 익명성이 사라진 컴퓨팅 환경의 도래(논의의 편리를 위해, DRM OS와 TCPA가 추구하는 컴퓨팅 모델을

TCB(Trusted Computing Base)라고 명명하자), 디지털저작권 보호를 위한 법률의 악용가능성^(1,9)이 가장 많이 연구되었다.

TCB의 핵심은 키를 생성하고 관리하며, 디지털 서명과 해쉬값을 계산할 수 있고, 키를 저장할 수 있는 비휘성 메모리를 갖춘 암호계산용 보조연산장치(cryptographic coprocessor)와 안전하다고 판단되는 프로그램만을 실행하게 할 수 있는 운영체계에 있다. 프라이버시에 대한 우려의 대응으로 암호계산용 보조연산장치에 저장된 키는 외부로 유출되지 않도록 설계되었다. 그러나, 식별 가능한 정보가 있다는 사실은 많은 DRM 시스템이 그 정보를 이용하는 방법(예, 주어진 데이터에 대한 해쉬값 계산)을 포함하려 할 것이고, 이는 사용자의 익명성을 훼손하게 될 것이다. 또한 어떤 프로그램이 안전한지를 판단한다는 것은 그러한 판단의 주체가 누구인가 하는 문제와 함께 어떻게 할 것인가 하는 문제가 야기할 것이다. 현재의 상황에서 볼 때 판단의 주체는 운영체제 제작자, 즉 Microsoft가 갖게 될 것이며, 방법으로는 운영체제 또는 하드웨어에 내재되어 있는 식별 가능한 정보를 이용할 것이다. 즉, TCB 환경에서는 사용자의 익명성이 보장되지 않는다.

TCB는 Microsoft와 Intel이 처음 주장하였듯이 2005년에 시장이 등장할 것으로 예상되지는 않지만 약 10년 이내에 서서히 등장할 것으로 예상된다. 그러나, 일반 사용자들의 반발과 점차 증가하는 비윈도우 컴퓨팅 환경이 큰 영향을 줄 것으로 예상된다. 일반 사용자의 반발은 운영체제시장에서 사실상 독점적 지배력을 가지고 있는 Microsoft에게도 분명 부담이 될 것이고, 이는 비윈도우 운영체제의 존재(예, 유닉스, Mac OS)와 윈도우 운영체제를 탑재하지 않은 기기(예: 핸드폰, PDA)를 이용한 인터넷 접속의 증가로 인해 더 큰 부담으로 Microsoft에게 작용할 것이다. 또한, TCB에 의해 통제되는 인터넷 환경이 일정부분 차지하겠지만 그러한 통제가 적용되지 않는 다른 환경이 존재할 것으로 예상된다⁽¹⁵⁾. 이러한 상황에서 통제된 환경을 따르느냐 또는 그렇지 않은 환경에 있는느냐는 개인의 취향과 함께 각 환경이 제공하는 서비스의 종류 및 질에 따라 결정 될 것이고, 각 사용자는 필요에 따라 두개의 환경을 넘나들며 이용할 것으로 예상된다.

한편, 디지털 저작권 보호를 위한 법률이 다른 목적으로 악용될 가능성에 대해서는 미국의 DMCA⁽¹⁾에 대한 사례를 중심으로 많은 논의가 있었다. 논란이 되고 있는 DMCA의 내용은 "DRM을 우회하는 방법을 개발하거나 그 방법을 공개하는 것은 불법"이라는 것이다. 그러나, 이

법률에 의한 실질적인 디지털 저작권 효과는 극히 미미하고, 사용자의 프라이버시, 정당한 사용권, 출판의 자유를 침해하는 사례가 빈번히 발생하여 문제를 야기하고 있다.

기술적 보호를 우회하는 행위를 불법으로 법제화 하는 경향은 현재 미국에 의해 주도되고 있다. 1996년 12월, 미국주도하에 열린 WIPO(World Intellectual Property Organization)에서 새로운 인터넷 환경에 대응하기 위한 외교회의가 개최되었고, 이 회의의 결과로 "저작권 보호를 위한 기술적 수단을 회피하거나 무력화시키는 장치, 도구 등의 제작, 수입에 대하여 법적조치를 취할 것을 규정"하였다. 이에 따라, 1998년 10월 미국은 DMCA를 제정하였고, 우리나라는 2001년 컴퓨터프로그램보호법에 WIPO의 내용을 첨가하였다. 아직까지, 우리나라에서는 구체적인 사례가 발생하고 있지는 않지만 앞으로 유사한 사례가 많이 발생할 것이고, 특히 미국과의 통상교섭과정에서 많은 논란이 있을 것으로 예상된다.

디지털 저작권에 대한 기술적 보호조치, 즉 DRM을 무력화하는 것을 금지하는 법안의 문제점은 법집행이 어렵다는데 있다. 현재, DRM 시스템들의 상당수는 약간의 프로그래밍 실력만 있다면 제거 가능한 것이고, 또한, 제거작업이 시도되는 기기(예, PC, 플레이어)는 개인의 소유인 경우가 많다. 이러한 상황에서, DRM 시스템의 무력화에 대한 처벌은 무력화방법이 타인에게 배포되는 경우에만 실질적인 집행이 가능한 것이다. 그러나, 이 경우에도 현재 인터넷을 통해 유포되는 형태를 고려해 볼 때 법적용은 사실상 불가능하다.

III. Privacy 향상 기술

DRM에서의 프라이버시를 향상하기 위한 여러 기술적 방법들이 제안되었다. 그러나, 서론에서 언급하였듯이 제안된 대부분의 방법들이 현실적 적용에 있어서는 많은 문제를 가지고 있다. 이 장에서는 PET의 문제점에 대해 살펴보도록 하자.

언뜻 보면, 암호를 이용하는 방법에 의해 DRM에서의 프라이버시 문제는 쉽게 해결 가능한 것으로 여겨질 수도 있다. DRM 관련 지불은 전자화폐를 이용하고, 인터넷 검색과 다운로드는 익명성이 보장되는 Mixnet(예, Anonymizer¹⁶⁾)를 이용하고, 자신에 대한 인증은 영지식 프로토콜 또는 안전한 함수계산(secure function evaluation)에 의해 익명성을 유지하는 방법 등을 이용하여 DRM에서의 프라이버시 문제는 쉽게 해결할 수 있을 것으로 희망하는 연구자들도 있지만, 그러한 희망이 현실과는 큰 차이가 있다.

현재, 제안된 DRM 관련 PET 기술들은 바로 앞에서 거론한 여러 방법들(예, 전자화폐, Mixnet, 영지식프로토콜)을 유기적으로 이용하는 방법이 주종을 이루고 있다. 그러나, 제안된 많은 PET 기술들은 국소적인 프로토콜에만 치중하여 전체적인 문제를 간과하는 경향이 많다. 이를, 구체적으로 살펴보면 다음과 같다.

- * 현실성의 결여 - 대부분의 PET 관련 암호 프로토콜에서는 신뢰할 수 있는 제 3자의 존재를 가정하고 프로토콜의 참여자간의 관계와 목적이 분명히 정의되어 있다. 그러나, DRM이 적용되어야 할 현실은 신뢰할 수 있는 제 3자가 존재하지도 않고 또한 법규에 의해 존재하게 한다 하여도 이를 위한 경제적 비용은 누가 책임질 것인가 하는 문제가 있으며, DRM 구성원(예, 사용자, 서비스제공자, 음원제공자, 저작권자, 창작자)간에 이해관계는 암호 프로토콜이 가정하는 것만큼 단순하지도, 분명하지도 않다.
- * 기술적 한계 - DRM은 여러 기술의 조합으로 이루어진 시스템으로, 주어진 DRM 시스템에서의 프라이버시 보호의 강도는 가장 약한 고리에 의해 결정될 것이다. 즉, 복잡하고 거대한 DRM 시스템에서 프라이버시 보호를 위해서는 아주 미세한 부분까지 고려해야 함을 의미한다. 이는 이론적인 프로토콜을 실제로 구현할 때 나타나는 여러 기술적 어려움을 고려해보면, PET의 국소적 해결책은 그 효용성이 적을 수밖에 없음이 쉽게 예상된다.

인터넷 검색에서의 프라이버시를 보호하기 위한 수단으로 자주 거론되고 있는 Mixnet(Remailer와 같이 Chaining 방식 등을 이용하여 인터넷 사용자의 익명성을 보장하는 기술, 예: Anonymizer)은 여러 기술적인 한계 때문에 DRM에서 가까운 장래에 이용되기에는 문제가 있다. 우선 Mixnet은 상당한 정도의 인터넷의 교통량(Traffic Bandwidth)을 차지할 것이다. 더 심각한 문제는 Mixnet에 의해 실질적인 익명성을 보장하기 위해서는 많은 수의 Mixnet hop이 필요할 것이고 이는 결과적으로 인터넷 교통패턴(Internet traffic pattern)의 변화를 초래할 것이다. 이러한 변화는 기존의 인터넷 교통을 원활하게 하기 위해 이용되고 있는 여러 기술들(예, Network load-balancing)을 방해하여 결국 전체적인 인터넷 이용에 큰 불편을 가져올 것이다.

- * 사용자의 행동양식 - 프라이버시 보호 관련하여 가장 통제가 힘든 DRM 구성원은 사용자가 될 것이

다. 많은 사용자들은 인터넷 이용에 있어서 프라이버시 침해 가능성에 대해 인지하지 못하거나 또는 그 중요성을 대수롭지 않게 여기는 경향이 많다. 프라이버시를 향상시킬 수 있는 여러 프로그램(예, 쿠키제거, Remailer, PGP)이 있으나 그것을 이용하는 사용자는 극히 적으며, 많은 사용자들이 프라이버시 보호를 위한 법률제정과 기술개발을 지원하는 태도를 취하지만, 실제, 자신의 프라이버시 보호를 위해서는, 간단한 절차도 편리함을 위해 무시하곤 한다.

일반적으로 DRM 서비스제공자에 대한 법률적인 규제 가 아닌 기술적인 방법에 의한 프라이버시 보호를 강화하면 할수록 해당 시스템에 대한 사용자의 편리성은 낮아질 것이다. 이 부분에 대해서 저자는 최소한 DRM 관련 프라이버시 보호는 많은 사용자들에게 편리성보다는 후순위로 여겨 질 것으로 예상된다. 기존의 DRM관련 PET 기술들은 사용자의 편리성에 대한 고려가 미약한 것이 문제이다.

- * 프라이버시 보호를 위한 경제적 비용 - 프라이버시 보호는 많은 경제적 비용을 요구한다. 바로 앞에서 거론한 사용자 편리성의 감소에 따른 경제적 비용 외에도, 프라이버시 보호를 위한 기술적 방법을 구현하는데 필요한 비용은 막대하며, 그것을 누가 부담할 것인가도 문제이다. 또한, 현실적으로 DRM 서비스 제공자는 저작권 보호 목적 외에도 인터넷을 통한 배급을 원활히 할 목적으로 사용자가 어떤 콘텐츠를 어떻게 요구하는지에 대한 정보를 필요로 한다. 이러한 것을 차단하는 것은 사용자의 불편을 가중시킬 것이다.

IV. DRM과 프라이버시의 조화

디지털 저작권 보호를 위한 기술 DRM과 프라이버시 보호를 위한 PET는 서로 상충되는 요소를 가지고 있고 이에 대한 기술적 해결은 요원하다. DRM은 저작권 보호를 위해 사용자를 식별할 수 있는 방법을 필요로 하고 PET는 프라이버시의 핵심인 익명성의 보장을 위해 사용자 식별을 할 수 없도록 또는 필요하지 않도록 하는데 노력을 집중하고 있다. 이러한 두 기술 사이의 상충되는 문제를 해결하는 방법으로 의미 있는 성공을 거둔 기술은 아직 등장하지 않았다.

이 글의 저자는 기술적 해결의 가능성이 요원한 상태

에서 취할 수 있는 방안으로 법에 의한 조정과 새로운 개념 정립을 통한 디지털 저작권과 프라이버시의 균형을 제시하고자 한다. 많은 디지털 저작권 옹호론자들은 기술적으로 완벽한 DRM과 우회금지조항과 같은 강력한 법률을 가장 효과적인 저작권 보호 수단으로 여기고 있다. 그러나, 실질적인 저작권 보호 효과, 즉, 저작권에 의한 경제적 혜택이 돌아가는 것은 기술적으로 완벽한 DRM과 강력한 법률에 크게 영향을 받고 있지 않다. 현재, 디지털 음악분야에서 상업적인 성공을 거두고 있는 DRM은 그 기술적 완벽성보다는 사용자 편리성에 더 강조한 점이 성공의 요인으로 여겨진다. 또한, 문제가 되는 DRM 시스템의 우회금지조항은 악용가능성이 높고 실제 적용에 있어서 여러 형태의 기술적 문제가 발생할 가능성이 높다. 실제로 미국에서 DMCA의 우회금지조항과 관련된 소송에서 대부분 저작권자들이 패소하였다.

실질적인 저작권 보호를 위해서는 편리한 DRM과 함께 불법복제를 줄이는 방법이 필요하다. 디지털 음악예로 불법복제의 종류와 그에 대한 대응방법을 살펴볼도록 하자. 여기서, 제안하고자 하는 대응방법은 프라이버시 침해가능성이 높은 사용자 식별이 필요하지 않는 것으로 실질적인 저작권 보호효과를 가져올 가능성이 높을 것으로 예상된다.

- * 물리적 복제 - CD-RW 등을 이용한 물리적 복제는 전파속도가 느리고 일반 개인들에 의해서 소규모로 이루어지는 경우가 대부분이다. 물리적 복제를 차단하는 기술과 법률 둘 다 적용이 힘들다. 그러나, 시간지연 있고 검색 가능한 음악 데이터베이스가 존재하지 않기 때문에 실질적인 저작권 피해는 상대적으로 적다.

- * 소규모 네트워크 - 자신의 홈페이지 등에 음악파일을 올려놓고 방문객으로 하여금 자유롭게 다운로드 하는 행위는 90년도 후반 일정기간동안 인터넷에 만연하였으나 현재는 대부분 사라지고 소규모의 그룹만이 이용할 수 있는 네트워크만이 남았다. 이러한 형태의 네트워크는 물리적 복제에 비해 시간지연은 상대적으로 단축되었으나 음악 데이터베이스의 크기는 인기음악을 중심으로 편중되어 있고 그 크기도 적다. 이러한 네트워크도 기술적으로나 또는 법에 의해 차단하기 힘들다. 이러한 이유에서 예상되는 인기도에 따라 다른 형태의 DRM을 적용하는 방법을 고려해 볼만 하다. 가령, 인기가 높을 것으로 예상되는 음악은 예약판매, 시간차 판매(예, Mobile 음악은 먼저 발매한 후에 CD를 나중에 발매하는 방

법) 등을 이용하는 것도 하나의 방법이 될 것이다.

* P2P 파일공유 - 1999년 Napster사는 P2P 기술을 이용한 파일공유 서비스를 시행하여 선풍적인 인기를 얻었지만, 음반사들은 저작권 침해(공유된 파일의 대부분이 mp3 음악파일이었음)를 이유로 소송을 제기하였다. 이에 대해 Naspetr측의 항변의 주요 내용은 자신들은 P2P 파일공유 서비스만을 제공할 뿐 실제 저작권을 침해하는 행위(자신의 음악을 타인에게 주거나 타인의 것을 받는 행위)는 사용자들에게 있다는 것이다. 이 소송의 결과는 Napster가 패소하여 파산하게 되었는데, 소송에 결과에 결정적 영향을 주었던 것은 Naspeter가 음악파일 이름에 대한 데이터베이스를 제공하였다는 것이었다. Napster 사건 이후에 등장하는 P2P 파일공유서비스는 파일이름에 대한 데이터베이스를 포함 모든 요소를 분산형을 취함으로써 기존에 문제가 되었던 저작권 침해주장을 피해 가고 있다.

분산형 P2P 파일공유의 약점은 소수의 사용자에 의해 음악파일이 제공되고 대다수의 사용자들은 단지 음악파일을 다운로드하는데 열중하고 있는 구조에 있다. 그러므로, 음악파일을 대량으로 제공하고 있는 소수의 사용자에 대한 법적제재(많은 경우, 해당 사용자가 속해 있는 회사나 대학에 경고문을 발송하는 것으로도 상당한 효과를 얻을 수 있다)를 통해서 P2P 파일공유에 의한 불법복제를 감소시킬 수 있을 것이다.

아날로그 시대에 음악에 대한 저작권이 누렸던 경제적 혜택은 기술의 발전에 기인하였다. 테이프, LP와 같이 저렴한 저장 매체와 재생기기의 등장, 그리고 TV와 같이 음악을 선전할 수 있는 수단 등 경제적 혜택의 원인은 기술의 발전에 있었다. 그러나, 현재는 기술의 발전이 도리어 방해가 되고 있는 상황이다. 현재의 저작권 보호를 강화한 DRM은 단지 사용자를 불편하게 할 뿐 저작권 보호 효과는 거의 전무하다. 실질적인 저작권 보호(이윤창출)는 편리성과 새로운 환경에 적합한 비즈니스 모델을 고려한 DRM에 의해 가능할 것이다. 즉, 디지털 저작권 보호기능보다는 콘텐츠 서비스 기능이 DRM의 더 중요한 부분이 되어야 한다.

DRM에서의 프라이버시 보호를 위해 가명(Pseudonym)을 이용한 서비스를 개발하고, DRM에서 필요로 하는 사용자 식별정보를 최소화하고 또한 안전하게 관리하는 것을 법제화해야 한다. 이러한 의미에서 P3P(Platform for Privacy Preferences)¹⁷⁾의 일부 내용을 DRM에 적용하는 법제화하는 것이 필요하다. 예를 들

어, DRM 서비스 제공자는 사용자에게 서비스 제공을 위해 사용자의 어떠한 개인 정보가 필요한지, 그 개인정보가 어떻게 이용되는지 등의 정보를 사용자에게 고지하고 준수하는 것을 의무화할 필요가 있다. 또한, 그러한 사항이 정확히 지켜지고 있는지 정기적인 감사(Auditing)를 받게 하는 것도 법제화해야 한다. 감사의 효과는 클 것으로 예상하는데 그 이유는 이러한 종류의 감사는 그 복잡도에 따라 감사비용이 결정되므로, 감사비용을 절약하기 위해서 DRM 서비스 제공자들은 최소한의 사용자 정보만을 스스로 요구할 가능성이 높기 때문이다.

상당수의 프라이버시 옹호론자들은 법이 아닌 기술에 의한 프라이버시 보호를 주장하고 있다. 그러나, 이러한 생각은 3장에서 살펴본 바와 같이 여러 기술적 문제와 함께 경제적 문제가 있다. 현재의 인터넷 이용 환경을 일시에 바꿀 만큼 프라이버시의 가치가 절대적이지 않으며, 또한 그러한 개혁이 가능하지도 않다.

V. 결 론

이 글의 목적은 디지털 저작권과 프라이버시 사이의 경합적 요인을 분석하고 대립되는 가치간의 균형을 위한 대안을 제시하는데 있다. 현재, 디지털 저작권보호를 위한 DRM 기술은 어느 정도의 사용자 정보를 요구하고 있고 이러한 사용자 정보는 유출될 경우 프라이버시 침해를 야기할 수 있다. 그렇다고 사용자 정보를 요구하는 것을 완전히 금지하는 것은 사실상 디지털 콘텐츠 시장의 붕괴를 초래할 위험이 있다.

프라이버시 보호를 위해 제안되어진 PET 기술의 상당수는 현재의 인터넷 이용환경에 적용하기에는 어려움이 많고 그 어려움을 해결하기 위한 전면적인 개혁은 그것을 할 수 있는 주체도 또한 기술도 존재하지 않고 있다. 이러한 상황에서 취할 수 있는 유일한 방법은 법에 의한 프라이버시 보호와 기술발전과 함께 진화해 가는 환경을 보다 더 프라이버시 친화적으로 바꾸려는 노력이 요구된다. 이러한 노력은 경제적 동기가 불분명하므로 자연적인 진화를 따르는 것은 힘들 것이다. 이러한 이유에서 프라이버시 친화적 환경은 법률에 의해 점진적으로 추진되어야 할 것이다.

DRM 서비스 제공자는 P3P와 유사한 형태의 프라이버시를 보호하기 위한 정책적 표준을 마련하고 그 표준에 대한 준수현황을 정기적으로 감사(Auditing) 받도록 의무화할 것을 제안한다. 또한, 사용자는 자신의 프라이버시를 지키기 위한 1차적인 노력을 기울여야 할 것이다.

참 고 문 헌

- [1] Electronic Frontier Foundation, "Unintended Consequences: Five Years under the DMCA", <http://www.eff.org/IP/DMCA>
- [2] J. Feigenbaum, M. Freedman, T. Sander, A. Shostack, "Privacy Engineering for Digital Rights Management System", <http://www.scs.cs.nyu.edu/~mfreed/docs/privacyeng-wspdrm01.pdf>
- [3] 김동원, "개인정보수집에서의 프라이버시와 경쟁가치들의 경합과 균형", *정보화정책*, 10(4), pp. 73-91, 2003
- [4] 신동룡, "저작권 확대 담론과 기술적 보호조치의 문제점에 관한 법철학적 연구", <http://myhome.hanafos.com/~lawphilo/krhomeall.htm>
- [5] E. Hughes, "A Cyberpunk's Manifesto", 1993. <http://www.activism.net/cypherpunk/manifesto.html>
- [6] N. Lundblad, "Privacy in a Noise Society", <http://www.sics.se/privacy/wholes2004/papers/lundblad.pdf>
- [7] P. Samuelson, "Digital Rights Management {and, or, vs} the Law", *Communications of the ACM* 46(4), 2001.
- [8] R. Stallman, "Right to Read", <http://www.gnu.org/philosophy/right-to-read.html>, 1997
- [9] <http://www.anti-dmca.org>
- [10] 박복녕, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시보호를 제공하는 라이선스 관리 프로토콜", *정보과학회논문지*, 30(2), pp. 189-198, 2003.
- [11] 최은영, 이동훈, 홍도원, "익명성을 보장하는 비대칭 공개키 공모자 추적기법", *정보보호학회논문지*, 14(3), pp. 49 - 61, 2004.
- [12] <http://www.sdmi.org>
- [13] DRM OS Patent, <http://cryptome.org/ms-drm-os.htm>
- [14] <https://www.trustedcomputinggroup.org>
- [15] P. Biddle, P. England, M. Peinado, B. William, "The Darknet and the Future of Content Distribution", 2002 ACM Workshop on Digital Rights Management. 2002.
- [16] <http://www.anonymizer.com>
- [17] <http://www.w3.org/P3P/>

〈著者紹介〉



이 남 용 (Nam-Yong Lee)

1990년 2월 : 서울대학교 수학과(학사)

1997년 12월 : Purdue University 수학과(박사)

2002년 9월~현재 : 인제대학교 컴

퓨터응용과학부 전임강사

〈관심분야〉 정보보호, 영상처리