Journal of Digital Convergence
Vol. 16. No. 9, pp. 159-172, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.9.159

온라인 트래킹 기술 분류 및 이용자 관점에서의 시사점

이보한[1], 나종연[2*]
[1]서울대학교 소비자학과 박사수료, [2]서울대학교 소비자학과 교수/서울대학교 생활과학연구소

Classification of Online Tracking Technology and Implications in User Perspective

Bohan Lee[1], Jong-Youn Rha[2*]
[1]Ph. D. Candidate, Dept. of Consumer Science, Seoul National University
[2]Professor, Dept. of Consumer Science, Seoul National University /
Research Institute of Human Ecology, Seoul National University

요 약 이용자의 정보를 수집하여 활용하는 온라인 트래킹 기술이 빠르게 발전하고 있다. 온라인 트래킹은 제품과 서비스 질의 향성, 이용자 경험의 증진의 측면에서 그 필요성이 강조되지만, 이용자의 프라이버시 침해나 정보 보안 취약성 등의 문제를 내포하고 있다. 이에 본 연구에서는 온라인 트래킹 기술들을 탐색하고, 이를 통해 온라인 트래킹과 관련한 정책 수립 시, 고려해야 할 사항을 파악하고자 하였다. 그 결과, 온라인 트래킹 기술은 '일반쿠키', '슈퍼쿠키', '핑거프린팅', '디바이스 ID 트래킹', '크로스 디바이스 트래킹' 등으로 구분되었다. 온라인 트래킹의 발생 단계, 기술 생성주체, 활용목적, 정보의 유지 기간 및 저장형식, 기술의 변화 등이 정책적으로 고려되어야 할 사항인 것으로 나타났다. 정책입안자와 산업관계자는 온라인 트래킹 기술의 특성에 따라 이용자가 인지하는 위험 정도가 다를 수 있음을 인지해야 한다. 그리고 온라인 트래킹 기술의 분류에 영향을 미칠 수 있는 다양한 요인에 대한 정책적인 이해가 필요하다. 마지막으로 산업계에서는 통합적 프라이버시 시스템을 구축 등의 선제적 대응이 필요하다.

주제어 : 온라인 트래킹, 매커니즘, 기술유형, 이용자보호, 소비자정책

Abstract This study searched and analyzed online tracking technologies. It tried to understand what to consider when establishing policies related to online tracking. Online tracking technologies were classified into 'general cookies', 'super cookies', 'fingerprinting', 'device ID tracking' and 'cross-device tracking'. Political considerations should include the layers of online tracking, the subjects of tracking technology, purpose of use, duration and storage format of information, and development of technology. The implications of this study are as follows: first, policy makers and industry should be aware that the degree of risk perceived by users may vary according to the characteristics of online tracking technology. Secondly, it is necessary to understand factors that affect the classification of online tracking technology. Finally, in the industry, preemptive measures such as building an integrated privacy system are needed to relieve anxiety of users and to build trust.

Key Words : Online tracking, Mechanism, Types of technologies, User protection, Consumer policy

*This study revised and supplemented the report of "Consumer Protection in the Era of Online Tracking: Suggestions for Improving Legislative Framework." by the Korea Internet & Security Agency.
*This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(NRF-2016S1A2A2912526).
*Corresponding Author : Jong-Youn Rha(jrha@snu.ac.kr)
Received June 14, 2018 Revised July 23, 2018
Accepted September 20, 2018 Published September 28, 2018

1. 서론

빅데이터 분석이 정교화 됨에 따라, 온라인상에서 이용자의 정보를 수집하여 활용하는 온라인 트래킹 기술이 빠르게 발전하고 있다[1]. 온라인 트래킹은 이용자의 정보를 활용함으로써 사회 전반의 편의와 효율을 증진시킬 수 있다는 점에서 주목받고 있다. 또한 이용자 입장에서도 온라인 트래킹으로 수집된 정보를 통해 각자의 취향과 관심에 기반하여, 보다 가치 있는 서비스를 제공받을 수 있기 때문에 효용성이 있는 기술이라 할 수 있다. 또한 이용자가 자주 활용하는 기능 등을 기억하여, 특정 작업을 빠르고 효율적으로 처리할 수 있도록 도움으로써 편의성을 증가시켜주기도 한다. 그러나 온라인 트래킹은 이용자가 트래킹이 일어나고 있다는 사실뿐만 아니라, 어떠한 정보가 수집되고 있는지 인지하지 못하는 프라이버시 문제를 내포하고 있다[2].

온라인 트래킹은 가장 보편적인 기술로 일컬어지는 '쿠키(Cookies)'뿐만 아니라 쿠키에서 진화된 형태인 '슈퍼 쿠키', 쿠키를 사용하지 않고도 이용자를 식별할 수 있는 '핑거프린팅(Fingerprinting)', 하나의 기기에 국한된 것이 아니라 서로 연결된 여러 기기를 트래킹 할 수 있는 '크로스 디바이스 트래킹(Cross-device tracking)'등 여러 형태로 나타나고 있으며, 이는 시간이 지날수록 고도화 되고 있다[3]. 이렇듯 온라인 트래킹 기술의 종류가 많아지고, 트래킹을 통해 정보를 수집하는 주체 역시 다양해지는 반면, 이용자는 이와 관련한 정보 습득이 용이하지 않고, 이용자 스스로가 원치 않는 온라인 트래킹을 통제하는 것이 어렵다[4,5].

실제로 2017년에 IBM에서 발표한 온라인 트래킹과 관련한 보고서에 따르면, 응답자의 약 64%가 이용자의 여러 가지 정보 중에서 어떠한 정보가 수집되고, 이용되는지 파악하기 어렵다고 답했으며, 약 96%의 응답자가 이용자가 정보 수집에 대한 통제권을 가져야 한다고 응답하였다[6]. 이는 이용자가 온라인 트래킹에 대해 정확히 이해하고, 이에 대응하기가 쉽지 않다는 점을 보여주는 결과이다. 온라인 트래킹 기술이 하루가 다르게 발전하고, 실질적으로 기술을 활용한 다양한 서비스가 제공되는 현 상황에서, 온라인 트래킹 기술이 가져올 수 있는 문제점들로부터 이용자를 보호하고, 개인정보처리자 및 수탁처리자 등을 포함한 다양한 이해관계자가 올바른 온라인 트래킹 행위를 수행할 수 있도록 하는 정책 환경을 조성하기 위한 연구가 활발히 이루어질 필요가 있다.

이러한 관심 속에서 온라인 트래킹과 같은 빅데이터 기술을 통한 이용자 정보 활용과 관련하여 사회적 논의가 시작되었다. 지난 2018년 2월, 4차산업혁명위원회는 빅데이터 산업 활성화의 기반이 되는 이용자 정보의 보호와 활용의 균형 방안 관련하여 규제·제도혁신 회의를 개최하였다. 그 결과, 이용자 정보의 개념을 크게 '개인정보', '가명정보', '익명정보' 등 3가지로 구분하고, 익명정보는 개인정보보호법 적용대상에서 제외하기로 결정하였다. 또한 가명정보의 개념과 보호 범위, 식별의 개념 등도 해외의 개인정보보호규정을 참고하여 정비해나가는 데에 합의하였으며, 법적 근거를 마련하기 위하여 관계부처가 이행 계획을 수립하고, 4차산업혁명위원회에서 이행 경과를 지속적으로 점검할 것을 밝혔다[7].

본 연구는 온라인 트래킹과 관련된 정책 수립에 있어서 이용자 관점에서 고려해야 하는 사항을 고찰하고자 한다. 이를 위해서는 온라인 트래킹 기술에 대한 이해가 필수적이다. 따라서 온라인 트래킹의 이해관계자와 작동 매커니즘을 파악하고, 다양한 온라인 트래킹 기술의 유형을 탐색하였다. 본 연구는 온라인 트래킹과 관련한 하나의 기술이 아닌, 다양한 스펙트럼의 기술을 포괄적으로 살펴보았다는 점에서 기존 연구와는 차별성을 가진다. 또한 온라인 트래킹의 위험으로부터 이용자를 보호함과 동시에, 신뢰할 수 있는 온라인 트래킹 산업 구축을 위한 정책적 초석이 될 수 있다는 점에서 의의를 지닌다.

2. 온라인 트래킹의 이해

2.1 온라인 트래킹의 정의

온라인 트래킹에 대한 국제 정책 기구의 정의를 살펴보면 다음과 같다. FTC(Federal Trade Commission)는 컴퓨터나 스마트폰 등을 포함하는 여러 디바이스에서 이용자 및 디바이스 정보를 수집(collect)하고, 저장(store)하며, 이러한 정보를 제 3자와 공유(share)하는 행위를 온라인 트래킹으로 간주하고 있다[8]. EU(European Union)은 이용자의 개인적인 행동이나 성향을 평가(evaluate)하거나 개인정보를 수집하여 분석(analyze)하고, 이를 기반으로 이용자의 향후 행동을 예측(predict)하는 자동화 된 개인정보 처리 과정을 온라인 트래킹이라고 설명하고 있다[9]. 유럽의회에 의해 설립되어 2004년

1월부터 활동을 이어오고 있는 유럽네트워크정보보호원(European Union Agency for Network and Information Security, ENISA) 역시 온라인 트래킹에 관한 보고서에서 사업자가 개인화·맞춤화된 서비스를 제공하고자 이용자의 웹 이용행태와 같은 데이터를 수집하고, 이용자의 관심사를 추론하는 일련의 과정을 온라인 트래킹으로 정의하였다[10].

우리나라의 경우, 온라인 트래킹과 관련한 명확한 정의를 내리고 있지는 않지만, 방송통신위원회에서는 온라인에서 이용자의 웹 사이트 방문 이력, 앱 사용 기록, 구매 및 검색 정보 등 관심이나 기호, 성향 등을 파악하는 것이 가능한 활동 정보 수집 행위를 온라인 트래킹으로 이해하고 있다[11].

앞서 살펴본 바와 같이 온라인 트래킹은 국내·외 기구에 따라 다소 상이하게 정의되었다. 그러나 온라인 트래킹에 대한 공통된 관점을 정리하면, 온라인 트래킹은 “사업자가 이용자에게 더 나은 제품 및 서비스를 제공하기 위하여 다양한 디바이스에서 유·무선 네트워크를 활용하여 개인정보를 수집·저장·공유하고 이를 평가·분석하며, 궁극적으로는 이용자의 관심을 추론하고, 미래 행동을 예측하는 일련의 행위”로 정의할 수 있다.

2.2 온라인 트래킹의 매커니즘

온라인 트래킹의 매커니즘을 이해하기 위해서는 이와 관련한 이해관계자에 대한 이해가 필수적이다. Fig. 1에서 볼 수 있듯이, 온라인 트래킹은 ‘광고주와 수요자 플랫폼(DSP, Demand Side Platform), 광고 네트워크(Ad Network) 및 광고 익스체인지(Ad Exchange), 마지막으로 공급자 플랫폼(SSP, Supply Side Platform)과 광고매체’라는 틀에서 이루어진다.

기존에는 광고주가 판매를 촉진하고자 하는 물품이나 서비스를 이용자에게 노출하기 위하여 다양한 매체에 광고를 의뢰하였다. 또한 광고 매체는 여러 지면에 광고를 실어주고 배포하면서 수익을 내는 구조를 형성하였다. 이용자는 광고를 통해 물품이나 서비스에 대한 정보를 얻기도 하며, 이는 직접적인 구매로 이어지기도 하였다. 그러나 광고의 영역이 온라인 중심으로 이동하면서 광고의 양이 폭발적으로 증가하여 이러한 구조는 더 이상 효율적으로 작동할 수 없게 되었다.

이러한 배경에서 등장한 광고 네트워크는 매체의 다양한 광고지면을 하나로 묶어 광고주에게 네트워크 단위로 제공한다. 이 때, 광고 네트워크는 온라인 트래킹을 이용하여 광고매체를 이용하는 이용자의 디바이스나 네트워크, 서비스 등에 관한 정보를 수집 및 분석한다. 광고 익스체인지는 광고 네트워크만으로 광고 수요와 공급을 원활히 이어주기 어렵기 때문에, 이들 간에 정보를 공유하는 플랫폼으로써 등장하였다. 광고 익스체인지 시스템에서는 이용자에게 노출된 광고의 유형과 시간이나 이용자와 관련한 정보 등의 수집이 더욱 집약적으로 이루어진다.

Fig. 2는 온라인 트래킹을 활용하는 쿠키에서 수집하는 정보의 예시이다. 예시에서 볼 수 있듯이, 광고 네트워

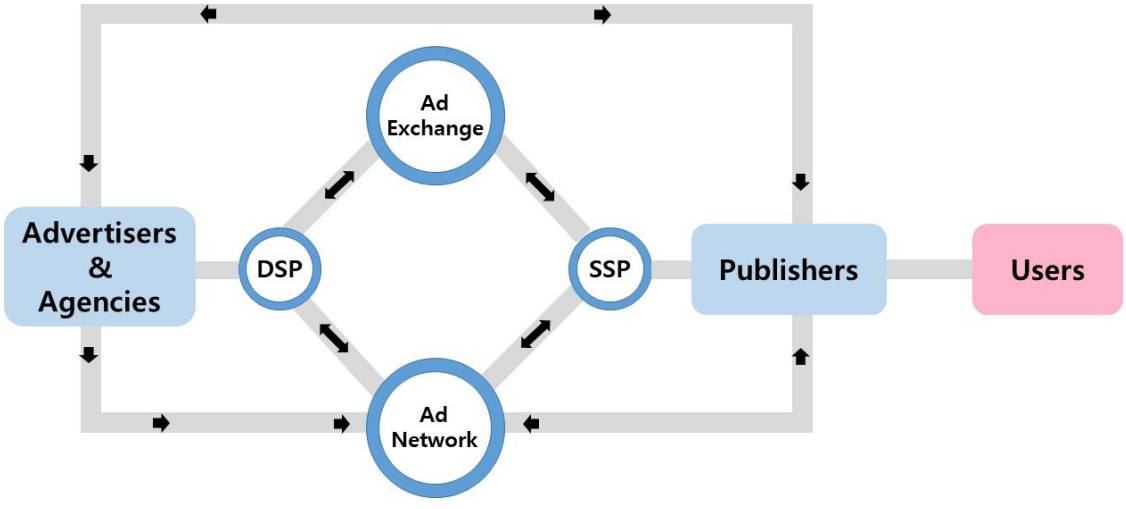

Fig. 1. Online Tracking Stakeholders and Operational Mechanisms

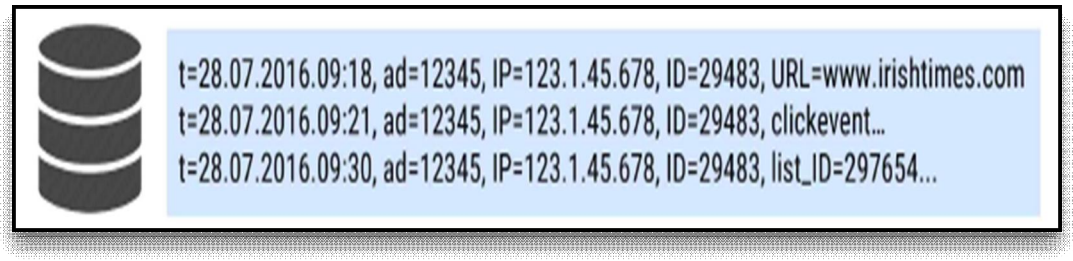

Fig. 2. an Example of Information Collected by Online Tracking Mechanism
(Source: Korea Onlinead Association. (2017). *Discussion about the development strategy of online advertising ecosystem using Big Data* (pp. 36-37))

크 및 광고 익스체인지는 광고 및 정보 전달의 효용성 높이기 위하여 이용자를 식별할 수 있는 다양한 장치를 활용하고, 온라인 트래킹을 통해 이용자의 행태 정보나 위치 정보를 수집한다. 또한 이러한 정보를 효과적으로 활용하기 위하여 이용자의 디바이스나 인터넷 브라우저 등에 심어둔 고유한 ID를 통해 이용자 혹은 디바이스를 식별한다[12].

수요자 플랫폼은 광고 네트워크나 광고 익스체인지를 통해 광고주가 효율이 높다고 판단되는 지면을 쉽게 구매할 수 있도록 돕는다. 공급자 플랫폼 역시 광고매체의 이익을 극대화하기 위해 광고 네트워크 및 광고 익스체인지와 상호작용한다. 광고매체는 이용자 정보를 활용하여 해당 이용자가 적절한 표적(target)인지 여부를 판단하고, 이용자에게 송출한다.

최근에는 온라인 트래킹이 진일보하여 프로그래머틱(programmatic) 방식으로 광고를 연결한다. 광고영역의 구매와 사용의 최적화를 위해 시스템 또는 프로그램으로 자동화한 방식이 프로그래머틱 방식이다. 프로그래머틱 방식은 모바일 광고 환경에 중요한 효율성과 속도에서 큰 장점을 갖고 있다. 타겟팅 기능을 다양하게 활용하면서도 개인화된 맞춤 광고를 신속히 내보낼 수 있다. 최근 이러한 방식을 활용하여 수요자 측면의 광고대행업체들이 실시간 경매 형태로 광고를 구매하고 최적화하는 작업을 실시하고 있다. eMarketer(2017)의 분석에 따르면, 2017년 광고 구매의 약 78%가 프로그래머틱 방식으로 이뤄지고 있다. 이는 광고를 이용자에게 신속하게 제공할 수 있다는 장점을 지니지만, 한편으로는 이용자 정보의 잘못된 분석으로 인해 피해를 유발할 수 있으며, 문제가 발생했을 때 책임 소지 역시 불분명해질 수 있다는 단점이 있다[13].

향후 정보통신기술 환경이 발달함에 따라 광고와 관련한 기술이 발전함에 따라 온라인 트래킹의 매커니즘 역시 복잡해지고, 규모 역시 확대될 것으로 예측된다.

3. 온라인 트래킹 기술 유형

3.1 쿠키

3.1.1 쿠키의 정의

쿠키란 웹사이트가 브라우저에 전송하는 '상태정보'를 저장하기 위한 것으로 이용자가 어떤 웹 사이트를 방문하면 등록한 이름, 방문한 사이트, 열람한 페이지, 특정 사이트에 등록한 비밀번호 등 이용자가 입력한 각종 정보가 저장되는 작은 텍스트 파일을 의미한다[14].

쿠키에 대한 정의는 시간이 흐름에 따라 변화의 조짐을 보이고 있다. 최근 FTC에 따르면, 이용자의 디바이스를 인식(recognize)하려는 목적을 가지며, 해당 사이트를 다시 방문했을 때, 저장된 정보를 읽어냄으로써 이용자를 구분(distinguish)할 수 있도록 하는 일련의 정보를 모두 쿠키로 간주하고 있다[15]. 즉, 쿠키란 이용자를 식별하기 위한 기술 및 정보만을 의미하는 것이 아니라, 이용자를 인식하고 구분하려는 목적을 가지는 모든 기술 및 정보를 일컫는다.

3.1.2 쿠키의 종류

본 연구에서는 쿠키를 오랫동안 활용되어 일반화 되어 있는 '일반 쿠키'와 이러한 일반 쿠키에서 진화·발전된 형태인 '슈퍼 쿠키(super-cookies)'라는 두 가지 카테고리로 나누고, 해당 범주를 구성하는 하위 쿠키들의 종류를 탐색하고자 하였다.

가. 일반 쿠키

일반 쿠키에 포함되는 첫 번째 쿠키는 '사이트 이용정보 쿠키'이다. 이는 웹사이트 내에서 이용자가 선호하는 설정을 기록하는 쿠키이다. 예를 들어 동영상 볼륨 설정, 게시물의 정렬순서 설정, 혹은 브라우저와 호환되는 비디오 스트리밍 속도를 기록한다. 이는 이용자가 다음에 이 웹사이트를 방문했을 때, 편리하게 이용할 수 있도록 도와주는 쿠키라고 할 수 있다.

두 번째, '등록 쿠키'는 이용자가 해당 웹페이지에 회원가입을 한 이후에 이용자의 로그인 기록을 저장하는 쿠키이다. 이용자가 어떤 계정으로 로그인했는지, 어떤 서비스 접근 권한을 갖게 되었는지, 해당 ID로 어떤 글을 올렸는지 정보를 저장한다. 로그인 이후에는 등록 쿠키와 분석 쿠키가 합쳐지며, 어떤 이용자가 어떤 페이지를 봤는지 더 많은 정보를 저장할 수 있게 된다. 쿠키가 개별적으로 존재했을 때에는 익명성을 유지할 수 있지만, 합쳐지게 되면 더 많은 정보가 저장된다는 점에 유의해야 한다.

세 번째, '분석 쿠키'는 웹사이트 접속자에 관한 통계분석을 위해 사용되는 쿠키이다. 이용자가 해당 웹사이트를 접속했는지 여부를 알려주며, 처음 방문하였다면 이 쿠키를 이용자의 브라우저에 심어진다. 이 쿠키를 통해 얼마나 많은 이용자가 해당 웹사이트에 접속하였는지, 얼마나 자주 방문하였는지에 관한 정보를 얻을 수 있다. 분석 쿠키는 익명으로 저장되어 개인을 구별해낼 수 없지만, 이용자가 해당 웹사이트에 로그인하면 더 이상 익명성을 유지하지 못하게 된다. 회원가입 시 제공한 ID, 이메일 주소와 같은 개인정보와 합쳐져, 개별 이용자의 웹사이트 접속 현황에 관한 정보를 통합적으로 저장하는 쿠키로 바뀌게 된다.

네 번째, '위치정보 쿠키'는 웹페이지 접속자의 국가정보를 저장하는 쿠키이다. 이용자가 웹페이지에 접속하면 브라우저에서 해당 웹페이지에 국가정보를 제공하고, 이는 익명으로 저장된다.

다섯 번째, '광고 쿠키'는 해당 웹페이지에서 특정 광고 유형을 보았는지, 광고를 본 시간이 어느 정도인지 등의 정보를 저장하는 쿠키로, 기본적으로 이용자가 방문한 웹 사이트에서 맞춤형 광고를 제공할 때 이용되는 쿠키이다.

마지막으로 '임시 쿠키'는 웹 사이트와 어플리케이션이 잘 이용되고 있는지 파악하고, 해당 페이지를 이용자 편의에 맞춰 제공하기 위해 작동한다.

나. 슈퍼 쿠키

슈퍼 쿠키는 이용자들이 탐지해내기 쉽지 않아 통제가 어려운 새로운 형태의 쿠키를 통칭하여 이르는 용어이다. 슈퍼 쿠키는 이용자가 웹사이트 방문기록(쿠키)를 삭제하더라도 어떤 사이트를 방문했는지 파악할 수 있다. 또한 일반적인 인터넷 쿠키와는 다른 위치(폴더)에 저장이 되기 때문에 이용자가 발견해내는 것 자체가 어려울 뿐 아니라 브라우저나 툴바에서 제공하는 일반 쿠키삭제 기능을 통해서는 삭제가 불가능한 특성을 지닌다.

슈퍼 쿠키의 문제점은 일반 쿠키의 경우, 각각의 웹 페이지에 따라 독립적으로 운영되지만, 슈퍼 쿠키는 2개 이상의 웹 사이트에 걸쳐 이용자의 활동정보를 수집할 수 있기 때문에 사이트 별로 상이한 자아(identity)를 유지하고자 하는 서비스 이용자의 의사에 반할 수 있다[16].

플래시 쿠키(Flash cookies)는 슈퍼 쿠키의 가장 대표적인 종류 중 하나이다. 플래시 쿠키는 인터넷 브라우저 플러그인인 어도비 플래시(Adobe Flash)를 이용함에 따라 발생하는 쿠키로, 로컬 공유 객체라고도 불린다. 어도비 사(社)에서 만든 플래시가 개인용 PC에 널리 보급되면서 알려졌으며, 이용자의 동영상 재생이 중단되거나 애니메이션 배너 광고가 멈춘 시점 등과 같은 플래시 관련 정보를 저장하며, 이용자가 클릭하지 않아도 실행된다는 특징을 지닌다. 일반 쿠키가 브라우저의 파일과 함께 저장되는 것과 달리, 플래시 쿠키는 별도의 어도비 파일에 저장되므로 어도비 플래시 플레이어(Adobe Flash Player) 설정을 통해 별도로 관리해야 삭제할 수 있다. 그러나 많은 이용자들이 플래시 쿠키가 존재한다는 사실을 모르고 있으며, 일반 쿠키를 삭제하더라도 플래시 쿠키는 지워지지 않는다는 것에 대해 알지 못한다[17]. 플래시 쿠키의 경우, 최대 100KB까지 정보를 수집할 수 있는데, 이는 일반 쿠키의 25배에 달하는 양이어서 이는 무분별한 개인정보 수집의 문제로 이어질 수 있다.

좀비 쿠키(Zombie cookies) 역시 슈퍼 쿠키의 일종이다. 좀비 쿠키는 일반 쿠키가 변형된 형태로, 이용자가 삭제를 하더라도 다시 재생성 되는 특징을 지닌 쿠키이다. 다시 생성되는 이유는 웹 브라우저 전용 쿠키 저장소가 아닌 다른 위치에 백업 파일이 존재하기 때문이다. 좀비 쿠키는 삭제하기 어려우며, 일반 쿠키에 의존하는 것이 아니기 때문에 쿠키를 삭제한 웹 브라우저에서도 동작할 수 있다. 일반적으로 좀비 쿠키는 앞서 설명한 플래시 기술에 기반한다.

3.2 핑거프린팅

핑거프린팅은 웹사이트를 보기 위해 사용하는 브라우저의 구성이나 설정 등을 기반으로 시간 경과에 따라 장치를 트래킹하는 방법으로, 쿠키를 사용하지 않고도 이용자를 식별할 수 있는 방법이다[4].

브라우저와 웹사이트를 운영하는 서버가 통신을 하는 과정에서 전송되는 기본정보에는 브라우저의 종류, PC의 운영체제(OS), 쿠키 사용여부(브라우저 설정값) 정보가 이용된다. 최근 웹사이트의 다양한 기능을 구현하기 위해 사용하는 어도비 플래시(Adobe Flash), 자바 가상머신(Java Virtual Machine)을 통해 브라우저 기능을 지원하는 프로그램의 버전, PC의 표준시, 화면 해상도, PC의 보유 글꼴 및 색상 등의 정보도 수집한다. 이처럼 브라우저가 서버와 통신하는 과정에서 발생하는 정보들이 모아져 브라우저 핑거프린팅이 된다[18]. 수집되는 정보 하나하나를 살펴보면 단순한 설정 정보이지만, 그 특징을 자세히 살펴보면 의미가 달라진다. 수집된 다양한 항목의 정보가 서로 조합되면 단순 설정 정보만으로도 이용자 식별이 가능하다[18].

핑거프린팅 정보는 쿠키차단이나 IP주소를 숨기는 프록시를 사용하더라도 수집할 수 있으며, 변경하려면 운영체제 및 소프트웨어의 정보를 변경해야 한다. 전자 프런티어 재단의 연구 결과, 쿠키 없이도 브라우저 지문을 통해 웹사이트 방문자 94%의 정보 수집이 가능한 것으로 나타났다. 판옵티클릭 사이트를 방문한 참가자들의 브라우저 470,161개에서 지문을 수집한 결과, 어도비 플래시나 자바 가상머신을 사용하는 경우는 방문자의 94.2%에서 브라우저 지문을 발견할 수 있었다. 이처럼 쿠키 설정을 해제하고 IP 주소를 숨기는 프록시를 사용해도 브라우저 핑거프린팅을 이용해 이용자의 정보는 트래킹 될 수 있다.

3.3 디바이스 ID 트래킹

스마트폰과 태블릿 PC가 보편화됨에 따라, 멀티 디바이스 환경 하에서 개별 이용자를 모두 식별하는 것은 상당히 어려워졌다. 따라서 기기에 부여된 고유한 ID를 통해 이용자가 아닌 디바이스를 식별할 수 있는 온라인 트래킹 기술이 등장하였다[19].

디바이스 ID는 전 세계의 모든 스마트 폰 또는 태블릿 PC를 식별하는 숫자 및 문자로 구성된 문자열이다. 디바이스 ID는 주로 모바일 장치에 저장되며, 다운로드 되어 설치된 모든 응용 프로그램에서 검색할 수 있게 된다. 모바일 앱은 일반적으로 디바이스 ID를 검색하여 서버와 통신 할 때, 디바이스를 확인하기 위하여 ID를 사용하게 된다.

모바일 광고의 맥락에서 디바이스 ID는 광고업자나 마케팅 담당자 등이 특정한 유형의 디바이스를 추적할 때 이용된다. 특히 대부분의 모바일 광고는 데이터를 기반으로 최적화 된다. 모바일 광고의 최적화 과정은 '광고의 집행 → 결과 트래킹 → 분석 → 최적화'로 진행되는데, 디바이스 ID를 통해서 이 모든 과정에 필요한 정보를 얻을 수 있다[20].

대표적인 디바이스 ID 트래킹 사례는 Google의 'AdID(Advertising ID)'와 Apple의 'IDFA(Identity For

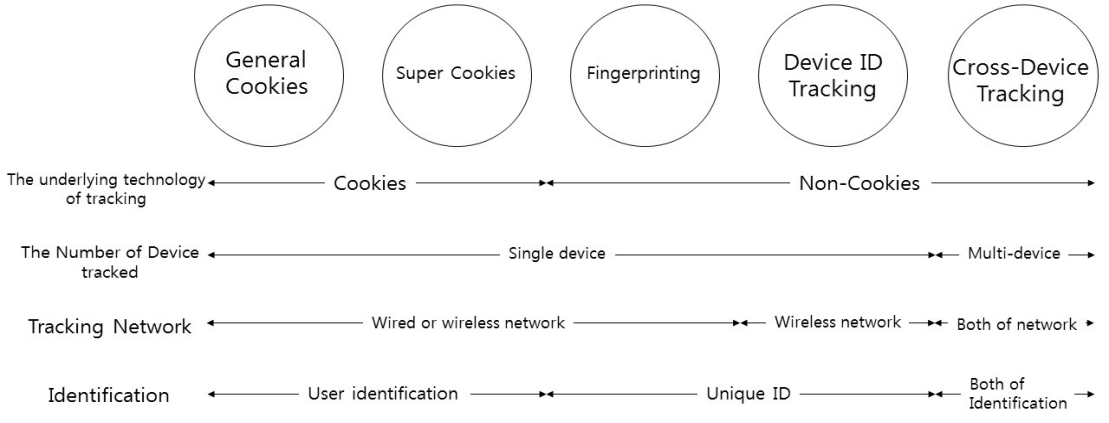

Fig. 3. Classification of Online Tracking Technologies

Advertisers)'이다. Google과 Apple은 각각 'Android ID'와 'UDID'라는 고유 단말기 식별번호가 있었으나, 개인정보 문제로 인하여 Apple은 2012년 iOS6 출시와 함께 'IDFA'라는 식별자를 내놓았고, Google 역시 2014년 8월 1일부터 'AdID'를 사용하고 있다.

Google의 AdID는 안드로이드 광고 어트리뷰션에 필요한 기기 식별자로 사용이 의무화되었다. Google의 AdID란 광고의 최적화 및 성과 분석 시 필요한 디바이스 ID 중 하나이다. 이 디바이스 ID를 기준으로 클릭 수, 노출도 등의 정보를 수집해 광고의 성과를 분석할 수 있으며, 광고의 성과에 대한 요인과 기여도 평가가 가능하다. 또한 AdID는 개발자에게는 간단하고 표준화된 시스템을 제공하며, 이용자에게는 Google 플레이에서 노출되는 광고를 컨트롤할 수 있도록 한다.

Apple의 IDFA는 모든 iOS 기기에 개발자와 마케팅 담당자가 광고 목적으로 활동을 추적할 수 있는 식별자를 일컫는다. IDFA는 Google의 AdID와 마찬가지로 이용자가 언제든지 재설정할 수 있으며, 이용자는 광고주가 IDFA를 이용해 맞춤형 광고를 제공하지 못하도록 제한하는 '광고 추적 제한'(Limit Ad Tracking)이라는 기기 설정을 사용하여 트래킹을 차단할 수 있다.

3.4 크로스 디바이스 트래킹

크로스 디바이스 트래킹은 결정론적(deterministic) 기법과 확률론적(probabilistic) 기법으로 나뉜다[21]. 결정론적 기법은 로그인과 같은 이용자 식별이 가능한 특성을 통해 디바이스와 관련한 이용자 정보를 트래킹한다. 결정론적 기법을 이용하여 수집한 이용자 정보를 둘러싼 프라이버시 이슈가 존재하며, 이 기법을 이용하는 사업자는 이용자의 정보를 보호할 책임이 있다.

크로스 디바이스 트래킹이 가능해지면서, 온라인 트래킹은 더 이상 하나의 디바이스에서만 일어나지 않는다. 사업자는 이용자에 대한 정보를 스마트폰, 태블릿, PC, 스마트 TV, 웨어러블 디바이스 등과 같이 서로 연결된 디바이스를 통해 수집할 수 있다. 또한 상당수의 사업자가 이러한 정보를 이용자의 오프라인에서의 습관 및 행태와 결합시키고자 한다[22].

반면, 사업자는 이용자가 서비스에 로그인하지 않은 경우에도 어떠한 이용자가 디바이스를 이용하는지 추론할 수 있는 확률론적인 접근법을 사용하기도 한다. 가장 대표적인 방식이 IP 주소를 일치시키는 것이다. 확률론적 기법은 각각의 디바이스에서 수많은 데이터 포인트를 수집하고, 디바이스 간의 연결성을 식별하기 위하여 복잡한 알고리즘을 이용한다. 이용자는 사업자가 확률적인 기법을 통해 트래킹할 때, 어떠한 서비스에도 로그인 할 필요가 없기 때문에 이러한 일련의 과정이 이용자에게 명백하게 제시되지 않을 수 있다.

앞서 살펴본 다양한 유형의 온라인 트래킹 기술을 '기반 기술', '트래킹 디바이스의 수', '트래킹 네트워크', '식별 내용' 등의 기준을 통해 분류해보면 Fig. 3과 같다.

4. 온라인 트래킹에서의 이용자 보호를 위한 정책적 고려사항

4.1 온라인 트래킹이 일어나는 단계(layer)

온라인 트래킹은 하나가 아닌, 여러 단계에서 다양하게 이루어진다[16]. 우선, 이용자가 사용하는 물리적인 '디바이스' 단에서 온라인 트래킹이 발생한다. 컴퓨터나 노트북, 스마트폰 및 태블릿 PC 등의 디바이스는 이용자가 네트워크에 접속하거나, 서비스를 이용하는 데에 도움을 주는 수단이다. 온라인 트래킹은 이러한 기기에 부여된 고유한 ID를 통해 이용자가 아닌 디바이스를 식별하고자 할 때 발생하게 되는데, 특히, 핑거프린팅이나 디바이스 ID 트래킹과 같은 형태로 일어난다[8]. 또한 최근에는 여러 가지 서비스를 다양한 디바이스를 활용하여 시간과 장소에 국한되지 않고, 동시다발적으로 이용하는 멀티 디바이스 환경이 도래함에 따라 크로스 디바이스 트래킹이 등장하여 진화하고 있다[23].

다음으로, 이용자에게 있어 '네트워크'는 물리적인 디바이스를 통해서 사업자가 제공하는 서비스를 이용하기 위해서는 필수적인 요소이다. 이 네트워크 단에서 이루어지는 온라인 트래킹을 통해 주로 네트워크 접속 시간 및 위치 등의 정보가 수집된다. 지난 2009년, 영국의 한 온라인광고 솔루션 업체에서 개발한 패킷감청기술이 영국, 미국 등에서 이용자의 프라이버시를 침해할 우려가 높다는 이유로 최종적으로 도입이 무산되는 사례가 있었다[24]. 이는 온라인 트래킹이 인터넷 서비스 제공자와 같은 네트워크 사업자에 의해서도 발생할 수 있음을 보여주는 사례라 할 수 있다.

마지막으로, 이용자에게 제공되는 '서비스' 단에서도 온라인 트래킹이 일어나게 된다[25]. 서비스 단에서는 이

용자가 이용하는 인터넷 브라우저나 모바일 어플리케이션으로부터 온라인 트래킹이 일어난다. 대표적인 사례가 2013년 12월과 2014년 11월, 각각 미국과 한국에서 발생한 '손전등 앱의 이용자 위치정보 수집'과 관련한 이슈이다[26]. 두 사건의 핵심은 이용자가 앱을 켤 때마다 위치정보와 단말기 정보 등을 수집하고 이를 제 3자에게 제공하였다는 점이다. 이는 사업자가 제공하는 여러 서비스에서 이용자가 인지하지 못하게 정보를 수집하고, 이를 공유하고 있음을 보여주는 사례라 할 수 있다. 또한 이용자가 이 사실을 알았다하더라도, 정보 수집·공유를 거부하면 앱을 더 이상 이용할 수 없게 된다는 점에서 이용자의 통제권을 제한한 경우라 볼 수 있다.

이와 같이 온라인 트래킹은 하나의 단계가 아닌 다양한 단계에 걸쳐 일어나고 있다. 따라서 각 단계에서 활동하고 있는 이해관계자(players)를 동일한 수준으로 규제해야 할지, 아니면 각각의 레이어 및 이해관계자의 특성을 고려해 서로 다른 수준의 규제를 적용할지에 대한 고민이 필요하다.

4.2 온라인 트래킹 기술의 생성주체

이용자는 온라인 트래킹 기술을 활용하는 주체에 따라 이에 대한 긴장(stress) 정도를 다르게 느낀다[27]. 이용자가 알 수 없는 제3의 주체에 의해 트래킹이 이루어지는 경우, 이용자와 직접적으로 관계를 맺은 대상에 의한 트래킹에 비해 심리적 압박이 크며, 이용자의 준비 혹은 대응 행동에 차이를 유발할 수 있기 때문이다.

온라인 트래킹은 그 생성주체에 따라서 당사자 트래킹(First-party tracking)과 제3자에 의한 트래킹(Third-party tracking)으로 구분할 수 있다. 당사자에 의한 트래킹은 이용자가 직접적으로 상호작용하고 있는 앱이나 방문 웹 사이트에서 활용되는 트래킹 기술이다. 제3자 트래킹은 이용자가 있는 사이트 이외의 주체가 배치한 기술로, 웹 사이트에서 특정 정보를 전달하기 위해 광고 네트워크와 제휴하거나 웹 사이트의 성과를 분석을 위해 분석회사에게 트래킹 정보를 제공할 수 있다. 제3자 회사는 이러한 온라인 트래킹 기술을 통해 시간흐름에 따른 이용자의 행동을 모니터할 수 있게 된다.

따라서 온라인 트래킹 기술과 관련한 정책을 수립할 때, 당사자에 의한 트래킹과 제3자에 의한 트래킹을 구분할 수 있는 기준과 더불어 규제 수위가 어떻게 달라야 할지 고려할 필요가 있다. 또한 '제3자'의 범위에 대한 명확한 규정과 어느 범위까지 규제를 적용할지에 대한 고민 역시 요구된다.

4.3 온라인 트래킹의 활용목적

활용목적에 따라 온라인 트래킹을 구분하는 것은 이용자가 웹 사이트를 이용하기 전, 해당 트래킹 기술이 어떠한 역할을 하는지 인지(recognize)하고, 이를 바탕으로 각 요소가 이용자 스스로에게 필요한지를 판단(judge)하여, 선택적으로 수용(accept)할 수 있게 하는 기준이 된다는 점에서 중요하다.

온라인 트래킹은 활용목적에 따라 필수적(necessary) 트래킹과 성능향상(performance)을 위한 트래킹, 기능성(functionality) 트래킹, 그리고 광고(advertising)를 위한 트래킹으로 구분할 수 있다[28].

영국의 British Telecom을 참고해보면, 필수적 트래킹 기술은 이용자가 웹 사이트를 방문하여 이용할 때, 반드시 필요한 기술을 일컫는다. 이러한 필수적 트래킹 기술 없이는 온라인 쇼핑이나 전자결제와 같은 서비스를 제공할 수 없게 된다.

성능향상 트래킹 기술은 이용자가 웹 페이지를 사용하는 방법에 대한 정보를 수집한다. 이용자가 가장 자주 방문하는 페이지와 웹페이지에서 발생하는 오류 메시지 등의 수집이 주를 이룬다.

기능성 트래킹 기술은 웹 사이트가 이용자가 선택한 이름, 언어, 지역 등을 기억할 수 있도록 한다. 또한 이용자의 변경 사항을 저장하여, 보다 개인화되고, 향상된 웹 사이트 특징을 구현하여 이용자에게 제공될 수 있도록 돕는다. 이 때, 수집하는 정보는 익명으로 처리되며, 다른 웹 사이트에서 발생하는 이용자의 인터넷 활동을 추적할 수 없다는 특징을 지닌다.

마지막으로 광고 트래킹 기술은 이용자 및 이용자의 관심에 더욱 관련된 광고를 전달하는 데에 사용된다. 또한 광고를 보는 횟수와 관련한 정보를 축적하고, 광고의 효과를 특정할 때 사용되기도 한다. 광고 관련 트래킹 기술은 다른 제3자에 의해 제공되는 사이트와 연결되는 기능을 포함하며, 이용자 개인의 인터넷 이용 습관을 구분할 수 있는 고유 값이나 다른 곳에 저장된 정보를 활용하여 이용자 선호를 파악하기도 한다[29].

온라인 트래킹과 관련한 정책에서는 활용목적에 따라 차등적인 규제가 필요할 것으로 보인다. 이용자가 서비스에 접근하여 활용하는 데에 필수적인 기술과 과도한

등장으로 이용자의 불만을 야기할 수 있는 광고 기술이 동일한 수준의 규제 대상이 되어서는 안 될 것이다. 따라서 정책의 방향과 수립에 있어 정보 활용 목적에 대한 고민은 규제 적용의 해당 유무와 그 강도를 결정하는 데에 있어 반드시 필요하다.

4.4 수집한 정보의 유지기간

이용자는 온라인 트래킹으로 의해 수집된 정보가 유지되는 기간에 따라 이에 관여하는 정도(involvement)가 달라질 수 있다. 이용자가 직접 삭제를 해야 되거나, 영구적으로 유지되는 트래킹 기술은 특정 기간 동안만 활성화 되었다가 사라지는 기술 유형에 비해 이용자의 관여도가 높으며, 그 수가 많을수록 이용자는 민감하게 반응하기 때문이다.

온라인 트래킹 기술로 수집에 정보는 유지기간에 따라 세션(session) 정보와 영구적(permanent) 저장 정보로 나눌 수 있다[30]. 세션 정보는 임시 저장 정보라고 불리며, 웹 사이트를 닫으면 지워지는 특징이 있다. 세션 정보는 임시 메모리에 저장되며 웹 브라우저를 종료한 후에는 유지되지 않는다. 또한 세션 정보는 이용자의 디바이스에서 수집된 정보가 아닌, 이용자를 식별하지 않는 세션 ID의 형태의 정보를 의미한다. 영구적 저장 정보는 만료될 때까지 이용자의 하드 드라이브에 저장되는 정보, 또는 이용자가 직접 삭제할 때까지 영구적으로 저장되는 정보를 의미한다. 영구적 저장 정보 또한 웹 서핑 동작이나 특정 웹 사이트의 이용자 기본 설정과 같이 이용자에 관한 식별 정보를 수집하는 데에 이용된다.

따라서 온라인 트래킹과 관련한 정책은 수집한 정보의 유지기간에 따라 기술을 구분하여 접근해야 한다. 보관기간이 상대적으로 길수록 규제와 감시를 통해 이용자가 삭제하고자 할 때 수집된 정보가 올바르게 폐기되도록 해야 한다. 또한 정보의 유효기간이 만료되었을 경우, 이용자에게 명확히 이를 고지하는지, 유지기간을 연장하고자 하는 경우, 이용자의 명시적 동의를 얻는지 등을 더욱 예의주시할 수 있는 방안을 모색해야 한다.

4.5 수집한 정보의 저장형식

온라인 트래킹 기술로 수집된 정보가 저장되는 형식은 이용자가 얻게 되는 편의성과 연관된다는 점에서 중요하다. 이용자의 행태와 관련한 정보를 더 많이 저장하여 이용자에게 더 빠르게 전달된다면 이용자의 효용이 증대될 수 있을 것이다.

이러한 저장형식의 변화가 일어나고 있는 대표적인 온라인 트래킹 기술이 바로 쿠키이다. 쿠키는 그 형식에 따라 HTTP 쿠키, 플래시 쿠키, HTML5 스토리지로 구분할 수 있다[31]. 각각의 특징을 정리해보면, Table 1과 같다.

HTTP 쿠키는 웹 쿠키, 브라우저 쿠키라고 불리며, 서버가 이용자의 웹 브라우저에 보내는 작은 데이터이다. 브라우저는 이를 저장하고 이후의 요청 사항(request)과 함께 서버로 다시 보낼 수 있다. 일반적으로 두 개의 요청 사항이 동일한 브라우저에서 왔는지 알려주는 역할을 한다. HTTP 쿠키의 크기는 4KB 이하이며, 기본 값(default)에서 정한 기한이 되면 만료되는 성격을 가진다.

플래시 쿠키는 로컬 공유 객체라고 불리는데, HTML5 스토리지 기술이 개발되기 전, HTTP 쿠키의 단점을 보완하고자 등장한 과도기적 성격의 쿠키이다. HTTP 쿠키와 비교하여 상대적으로 덜 알려져 있고, 이용자가 삭제하기 더욱 어려우며, 트래킹에 효과적이라는 특징을 가진다[32]. 또한 HTTP 쿠키에 비해 그 유지기간이 길고, 그 크기 역시 100KB로 25배 크다.

HTML5 스토리지는 Flash 쿠키와 달리 플러그인을 사용하지 않아도 되기 때문에 가장 보편적인 트래킹 매커니즘이 될 것으로 평가받는다. 또한 HTTP 쿠키는 서버로 전송되지만, HTML5 스토리지의 데이터는 서버와의 통신을 거치지 않아도 되기 때문에 빠르게 정보를 전달할 수 있으며, 네트워크 트래픽이 감소하는 효과가 있다. HTML5 스토리지는 만료기한이 없어 이용자가 삭제

Table 1. Key features of HTTP cookies, Flash cookies, and HTML5 storage

	HTTP cookies	Flash cookies	HTML5 Storage
Size	4KB	100KB	5MB
Saved location	SQL files	Non-browsers	SQL files
How to access	Accessible through a single browser	Accessible through various browsers on the same device	Accessible through a single browser

하기 전까지 유지되는 영구적 속성을 지니며, 그 크기 또한 5MB로 HTTP 쿠키나 Flash 쿠키에 비해 비약적으로 용량이 증가하였다[33].

온라인 트래킹에서 이용자의 정보를 저장하는 형식은 진화를 거듭하고 있다. 따라서 지속적으로 증가하고 있는 이용자 정보 저장 용량에 대한 합리적인 기준 에 대한 합의가 필요하다. 또한 정보를 저장하는 공간의 안전성과 접근 방식의 적절성에 대한 논의 역시 요구된다.

4.6 기술의 변화

앞서 논의된 크로스 디바이스 트래킹은 최근 기술의 변화를 반영한 대표적 사례이다. FTC(2017)에서는 크로스 디바이스 트래킹은 이용자와 사업자 모두에게 기회로 작용할 수 있지만. 이와 관련한 여러 우려도 표명하고 있다[8].

크로스 디바이스 트래킹은 이용자가 다양한 디바이스를 사용함에 있어 끊김없는 자연스러운(seamless) 경험을 할 수 있도록 하며, 사업자로 하여금 이용자에게 더 나은 온라인 경험을 제공할 수 있도록 도움을 줄 수 있다. 또한 크로스 디바이스 트래킹을 통해 사기 범죄를 탐지하고, 이용자 계정의 안전이 개선될 수 있다. 더 많은 거래가 온라인에서 일어남에 따라, 사업자는 이용자가 새로운 디바이스를 사용하여 자신의 계정에 접근할 때, 또 다른 디바이스를 통한 추가 인증을 진행함으로써 계정이 다른 이용자에 의해 부당하게 이용되고 있는지 여부를 확인할 수 있기 때문이다.

하지만 FTC는 크로스 디바이스 트래킹이 직면한 문제점에도 주목하고 있다. 첫 번째는 투명성의 문제이다. 크로스 디바이스 트래킹은 가시적이지 않기 때문에 이용자는 특정 디바이스에서의 행동이 또 다른 디바이스에서 등장하는 광고와 연결되었다는 사실에 불편해할 수 있다. 특히 이용자가 서비스에 로그인하지 않고도 트래킹 될 수 있는 확률론적 기법은 민감한 정보가 관련되어 있는 경우, 이용자 불만을 야기할 가능성이 크다고 지적한다. 또한 새로운 기술에 불안감을 가지는 이용자가 크로스 디바이스 트래킹을 통제할 수 있는 선택의 폭은 제한되어 있는 편이다. 즉, 이용자가 기존의 온라인 트래킹 기능을 사용하지 않도록 할 수 있는 역량이 증가한다고 하더라도, 크로스 디바이스 트래킹에는 적용할 수 없는 부분이 존재한다. 마지막으로, 크로스 디바이스 트래킹은 보안과 관련한 문제가 발생했을 때 취약할 수 있다. 확률론적인 기법을 이용한 추론을 위해서는 방대한 양의 브라우징 및 앱 데이터를 수집하고 이용되기 때문이다. 더욱이, 이용자 정보를 저장하는 제3자 아카이브가 침해당하면, 지식 기반 인증(knowledge-based authentication)과 같은 추가적인 보안 조치가 제 기능을 상실할 수 있다.

크로스 디바이스 트래킹과 같은 기술의 변화를 고려했을 때, 4차산업혁명위원회가 통계나 분석형태의 정보인 '익명정보'를 개인정보보호법 대상에서 제외하여 개인정보와 분리하기로 한 결정은 정책적 측면에서 다시 생각해보아야 할 문제이다. 빅데이터 분석을 기반으로 하는 새로운 온라인 트래킹 기술은 기본적으로 방대한 양의 이용자 정보를 수집·분석한다. 따라서 개인을 식별할 수 없는 익명의 정보라고 할지라도, 분석 과정에서 정보가 모여 다양한 형태로 결합하면, 확률적으로 개인을 식별해내는 것이 가능해진다[34,35]. 따라서 이러한 문제를 미연에 방지하기 위해 기술의 변화에도 선제적으로 대응할 수 있는 정책에 대한 고민이 요구된다.

4.7 소결

Fig. 4는 앞서 살펴본 여러 가지 정책적 고려사항에 따라 온라인 트래킹 기술을 구분하고, 이를 통한 온라인 트래킹의 위험 정도의 스펙트럼으로 보여주고 있다. Fig. 4가 의미하는 바는 온라인 트래킹이 반드시 규제의 대상이 되어야 한다거나 이용자를 무조건적으로 보호해야 한다는 것이 아니다. 오히려 이용자가 웹 사이트나 앱을 이용하는 데에 있어 반드시 필요하고, 이용자의 편의와 효용을 증대시켜주는 온라인 트래킹 기술이 존재할 수 있다는 점 역시 발견된다. 다만, 특정 지점을 지나게 되면, 더 많은 주체가 온라인 트래킹에 관여하고, 이용자의 관여도가 높아지며, 기술이 발달하여 이용자가 이를 탐지하여 삭제하거나 통제하기가 어려워짐에 따라 그 위험정도가 증가하게 될 수 있음을 보여준다.

온라인 트래킹과 관련한 기술들은 시간이 지남에 따라 더욱 복잡·세분화되고, 기존의 기술이 새로운 모습으로 진화하고 있다. 또한 그간 존재하지 않았던 새로운 형태의 기술이 계속해서 등장하기도 한다. 이렇듯 정보통신기술(Information and Communication Technology, ICT) 환경이 변화를 거듭하고 있고, 멀티 디바이스 이용이 보편화됨에 따라 온라인 트래킹 기술의 양태는 다양화 되고 있다는 점에 주목할 필요가 있다.

다만, 온라인 트래킹 관련 정책은 새로운 기술로 인해

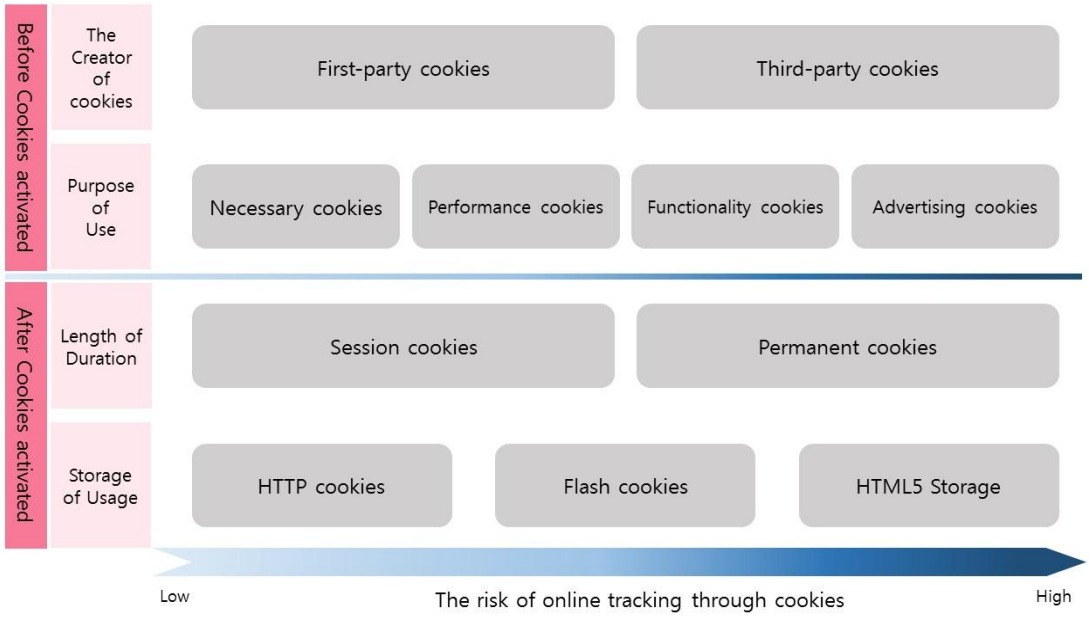

Fig. 4. Risk spectrum according to cookie classification

발생하는 문제도 중요하게 고려해야 하지만, 기존의 기술 변화 역시 대처할 수 있어야 한다. 다양한 온라인 트래킹 기술이 등장하고 있는 현 시점에서, 새로운 온라인 트래킹 기술의 등장에 정책적 관심이 편중되지 않도록 주의할 필요가 있다. 쿠키와 같은 가장 보편적인 기술 역시 빠르게 진화하고 발전하고 있으므로 이에 대한 대응 방안도 여전히 중요하다.

5. 결론

이용자의 정보를 수집하여 분석하는 기술이 빠르게 발달하면서, 온라인 혹은 모바일 이용자의 활동 정보를 추적하고 광고와 마케팅 등 상업적 목적으로 활용하는 온라인 트래킹 활동은 앞으로도 지속될 전망이다.

최근 발표된 4차산업혁명위원회의 기조 역시 위와 같은 온라인 트래킹의 장·단점 및 특성을 고려하여 정책적 접근을 시도하는 것으로 해석된다. 무조건적인 이용자 보호나 조건 없는 신산업 육성이 아니라, 이용자 정보 활용에 대한 요구와 필요성을 인지하면서도 프라이버시 침해와 같은 위험에서 이용자를 보호할 수 있는 정책이 필요함을 주장하고 있다. 이를 통해 이용자 정보의 활용과 보호의 조화를 도모하고, 안전하면서도 효율적인 산업 기반을 조성하고자 한다. 다만, 4차산업혁명위원회는 통계나 분석형태의 정보인 '익명정보'는 개인정보보호법 적용대상에서 제외하기로 결정하였는데, 이는 크로스 디바이스 트래킹과 같이 확률론적 기법의 분석 기술이 등장하는 시점에서 재고해볼 필요가 있다. 수집한 이용자 정보가 방대해지고, 이를 알고리즘을 통해 결합했을 때 이용자의 습관이나 행태와 관련한 무궁무진한 추론이 가능해지고, 결과적으로 이용자 피해까지 발생할 수 있기 때문이다[36].

본 연구에서는 온라인 트래킹에 대한 논의의 시의 적절성을 인지하고, 보다 깊은 고찰을 위해 온라인 트래킹 기술 현황을 전반적으로 탐색하였다. 이를 통해 온라인 트래킹 기술을 특징에 따라 분류하고, 온라인 트래킹과 관련한 정책 수립에 있어 고려해야 할 사항을 논의하였다. 정보통신기술 환경 변화와 멀티 디바이스 이용의 보편화라는 환경적 변화에 비추어 볼 때, 본 연구는 다음과 같은 정책적·산업적 의의를 갖는다.

첫째, 정책입안자 및 산업관계자 모두 온라인 트래킹 기술의 특성에 따라 이용자가 인지하는 위험 정도가 상이할 수 있음을 고려해야 한다. 온라인 트래킹 활용 주체가 이용자가 직접적으로 관계를 맺고 있는 이해관계자가 아닌, 알 수 없는 제3자인 경우, 이는 이용자에게 심리적으로 더 큰 압박을 주게 된다. 온라인 트래킹을 통해 수

집된 정보의 양이나 유지기간도 마찬가지이다. 정보를 저장할 수 있는 크기가 커지고, 수집되는 정보의 양이 늘어날수록, 이용자의 관여도가 높아지고, 트래킹 행위에 민감해진다. 또한 온라인 트래킹의 대상이 되는 주체에 따라서도 이용자가 인지하는 위험의 정도가 달라질 수 있다. 쿠키와 같은 기술은 '이용자'의 행태 정보를 수집하는 반면, 최근 핑거프린팅이나 디바이스 ID 트래킹의 경우, 이용자가 아닌 '디바이스' 정보를 추적하게 된다. 이용자가 온라인 트래킹을 통한 정보 수집을 인지하기 더욱 어렵게 하며, 이로 인해 이용자의 불안은 증가하게 된다. 더욱이 최근에는 크로스 디바이스 트래킹을 통해 이용자 정보와 디바이스 정보를 결합하여 새로운 정보를 생성하는 기술이 발달함에 따라 이용자가 느끼는 위험 수준은 커질 것으로 예상된다. 다만, 본 연구에서 살펴본 바와 같이, 이용자는 온라인 트래킹 기술 모두가 위험하다고 느끼거나 부정적인 태도를 가지진 않는다. 실제로 이용자는 그들의 편의를 제고하고, 서비스를 이용하는 데에 필수적인 기술에 대해서는 오히려 온라인 트래킹을 허용할 의향을 보이기도 하였다[37]. 중요한 점은 이용자 관점에서의 온라인 트래킹은 이분법적인 사고에서 벗어나 기술의 특성에 따라 이용자가 인지하는 위험성에 스펙트럼이 존재한다는 것이다.

둘째, 정책적 시각에서 볼 때, 온라인 트래킹 기술 유형을 분류하는 데에는 복합적이고 다양한 요인(factor)이 존재하므로, 이에 대한 고려가 필요하다. 온라인 트래킹의 양상은 이용자의 서비스 이용 맥락에 따라 다양한 모습을 띠게 된다. 온라인 트래킹은 역동적으로 이루어지고 있으며, 그 정도와 양태에 영향을 미치는 요인 또한 다양하다. 이러한 상황에서 온라인 트래킹 기술을 군집화 하여 분류하는 작업은 유의미하다고 할 수 있다. 그러나 시간이 지날수록 새로운 온라인 트래킹 기술이 등장할 때마다 그 특성을 파악하여 유형을 분류하는 것은 쉽지 않다. 기존의 기술까지 더해져서 분류 자체가 거대해진다면, 유형화의 효율성도 떨어진다. 따라서 온라인 트래킹 기술의 유형화와 더불어, 보다 근본적인 접근이 필요하다. 즉, 유형화에 있어 고려되어야 할 여러 기준이 존재한다는 점을 인지하고, 기술을 분류할 수 있는 요인이 무엇인가에 대한 고민이 더욱 요구된다. 본 연구에서는 온라인 트래킹 행위의 주체가 누구인지, 또한 그 행위의 목적은 무엇인지가 기술을 분류하는 기준이 될 수 있다고 판단하였다. 이와 더불어 해당 온라인 트래킹을 구성하는 기반 기술, 수집한 정보의 양와 보유 기간 역시 중요한 요인이 된다. 또한 향후 온라인 트래킹 기술 분류에 있어 '식별 대상'은 중요한 요인이 될 것으로 보인다. 크로스 디바이스 트래킹 등으로 이용자뿐만 아니라 그들이 이용하는 디바이스가 추적 대상이 되고 있기 때문이다. 따라서 이용자를 위한 정책적 접근은 특정 기기에 한정되지 않고 추후 다양한 형태의 기기(IoT, 웨어러블 기기 등)가 활용될 환경 역시 고려되어야 한다.

셋째, 산업적 측면에서는 온라인 트래킹에 대한 이용자의 불안감 해소 및 신뢰 형성을 위한 선제적 대응이 필요하다. 이와 동시에 온라인 트래킹의 전체적인 프로세스에서 이용자를 보호하고, 그들의 통제권을 보장할 수 있는 통합적인 대처가 요구된다. 온라인 트래킹과 관련한 산업계에서는 스스로가 기술의 디자인 단계부터 이용자의 권익을 고려하는 자세를 가질 필요가 있다. FTC가 2012년 보고서에서 제안한 '프라이버시 바이 디자인(Privacy by design)'이 대표적인데, 이 개념은 프라이버시 침해에 대한 위험을 줄이기 위해 시스템 개발에서부터 사전에 프라이버시를 고려하는 접근법으로, 전체 시스템 엔지니어링의 주기(cycle)에 걸쳐 일관되게 프라이버시를 고려하여 실시하는 것을 의미한다[38]. 즉, 산업적 측면에서 온라인 트래킹에 따른 문제가 발생한 후 이를 해결하는 것이 아니라, 능동적인 주체로서 서비스의 디자인과 개발, 실제 활용 및 사후에 이르기까지 전 단계에서 이용자 보호를 위해 노력해야 한다. 이와 더불어, 온라인 트래킹을 통해 활용되는 정보 역시 그 양과 종류가 많기 때문에, 이용자가 그 내용을 정확하게 인지하지 못할 수 있다. 또한, 서비스의 내용 및 서비스에 관계된 이해관계자의 다양성 등에 따라 온라인 트래킹의 정도가 달라질 수 있다. 더욱이 이용자가 처음 접하는 웹 사이트와 네비게이션을 해 나가면서 접하는 추가적인 웹 사이트에서의 온라인 트래킹의 정도가 다를 수도 있다. 따라서 온라인 트래킹의 정도와 내용에 대한 정보를 이용자에게 어떻게 정확하게, 동시에 이용자 관점에서 직관적이고 편안하게 전달할 수 있는지에 대한 산업적인 고민이 요구된다.

REFERENCES

[1] W. Meng, B. Lee, X. Xing & W. Lee. (2016). Track me or not: Enabling flexible control on web tracking. In

Proceedings of *the 25th International Conference on World Wide Web,* 99-109.

[2] J. C. Havens. (2015). Hacking happiness: Why your personal data counts and how tracking it can change the world. *TarcherPerigee.*

[3] J. Brookman, P. Rouge, A. Alva & C. Yeung. (2017). Cross-device tracking: Measurement and disclosures. *Proceedings on Privacy Enhancing Technologies, 2017(2),* 133-148.

[4] S. Englehard & A. Narayanan. (2016). "Online tracking: A 1-million-site measurement and analysis." In Proceedings of *the 2016 ACM SIGSAC Conference on Computer and Communications Security.* 1388-1401.

[5] S. Hong & H. Sin. (2017). Analysis of the Vulnerability of the IoT by the Scenario. *Journal of the Korea Convergence Society, 8(9),* 1-7.

[6] B. Fox, N. Gurney, & M. Cavestany. (2017). The trust factor in the cognitive era: How CSPs can capitalize on personal data while preserving privacy, *IBM Institute for Business.*

[7] PRESIDENTIAL COMMITTEE ON THE FOURTH INDUSTRIAL REVOLUTION. (2018). *Discussions on the revitalization of various digital signatures through amendment of electronic signature law.* Seoul: 4th-IR

[8] Federal Trade Commission. (2017). Cross-Device Tracking. *staff report, Jan. FTC.*

[9] A. Kolah. (2018). The GDPR Handbook: A Guide to the EU General Data Protection Regulation, *Kogan Page.*

[10] C. Castelluccia & A. Narayanan. (2012). Privacy considerations of online behavioural tracking. *European Network and Information Security Agency (ENISA).*

[11] Korea Communications Commission. (2017). *Online Personalized Ad Privacy Guidelines.* KCC.

[12] Korea Onlinead Association. (2017). *Discussion about the development strategy of online advertising ecosystem using Big Data.* Seoul: Korea Onlinead Association.

[13] eMarketer. (2017). Net Digital Ad Revenue Share Worldwide, by Company, 2016-2019. *eMarketer(Online).* http://www.emarketer.com/Chart/Net-Digital-Ad-Revenue-Share-Worldwide-by-Company-2016-2019-of-total-billions/205364.

[14] A. M. Hormozi. (2005). Cookies and privacy. *EDPACS, 32(9),* 1-13.

[15] Federal Trade Commission. (2016). Internet Cookies. *FTC(Online).* https://www.ftc.gov/site-information/privacy-policy/internet-cookies

[16] C. Castelluccia. (2012). Behavioural tracking on the internet: a technical perspective. In European Data Protection: In Good Health? (pp. 21-33). *Springer,* Dordrecht.

[17] A. Soltani, S. Canty, Q. Mayo, L. Thomas & C. J. Hoofnagle. (2009). Flash cookies and privacy. *SSRN Electronic Journal,* 1-8.

[18] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, P. Piessens & G. Vigna. (2013, May). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. *In Security and privacy (SP), 2013 IEEE symposium on* (pp. 541-555). IEEE.

[19] K. Takeda. (2012, October). User Identification and Tracking with online device fingerprints fusion. *In Security Technology (ICCST), 2012 IEEE International Carnahan Conference on* (pp. 163-167). IEEE.

[20] S. Seneviratne, H. Kolamunna & A. Seneviratne. (2015, June). A measurement study of tracking in paid mobile applications. *In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (p. 7). ACM.

[21] J. C. Havens. (2015). Hacking happiness: Why your personal data counts and how tracking it can change the world. *TarcherPerigee.*

[22] S. Zimmeck, J. S. Li, H. Kim, S. M. Bellovin, & T. Jebara. (2017, August). A privacy analysis of cross-device tracking. *In 26th USENIX Security Symposium* (USENIX Security 2017).

[23] Network Advertising Initiative. (2018). 2018 NAI Code of Conduct. *NAI.*

[24] Financial News. (2009). *The Korea Communications Commission (KCC) will make an online ad customization guide within the year.* fnnews. http://www.fnnews.com/news/200910121814269647?t=y

[25] R. K. Sar & Y. Al-Saggaf. (2014). Contextual integrity's decision heuristic and the tracking by social network sites. *Ethics and Information Technology, 16(1),* 15-26.

[26] G. Bae, Y. Lee, E. Kim, G. Tae, H. Kim & H. Lee. (2018). Detection of Android Apps Requiring Excessive Permissions. *Korea Society of Computer Information, 26(1),* 79-80.

[27] J. Pierson & R. Heyman. (2011). Social media and cookies: challenges for online privacy. *info, 13(6),* 30-42.

[28] British Telecom. (2018). More about cookies on BT.com, *BT(Online).* *https://home.bt.com/pages/cookies/more-about-cookies.html*

[29] J. Lee & J. Rha. (2015). How Consumers Perceive Online

Behavioral Advertising : Consumer Typology and Determining Factors. *Journal of Digital Convergence, 13(9),* 105-114.

[30] British Broadcasting Corporation. (2016). What do I need to know about cookies?. *BBC(Online). http://www.bbc.com/usingthebbc/cookies/what-do-i-need-to-know-about-cookies*

[31] M. G. CIP. (2015). The cookie trail: Why IG pros must follow the crumbs. *Information Management, 49(2),* 24.

[32] M. Ayenson, D. Wambach, A. Soltani, N. Good & C. Hoofnagle. (2011). Flash cookies and privacy II: Now with HTML5 and ETag respawning.

[33] I. Derksen, I. E. Poll & F. van den Broek. (2016). HTML5 Tracking Techniques in Practice. *Radboud University.*

[34] K. Crawford & J. Schultz. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev., 55*, 93.

[35] H. Kong, H. Jun & S. Yoon. (2018). A Study on the Privacy Policy of Behavioral Advertising. *Journal of the Korea Convergence Society, 9(3)*, 231-240.

[36] J. Rha. (2014). Legal issues of privacy; Suggestions for collecting and using consumer-oriented personal information. *BFL, 66*, 53-66.

[37] ThreatMetrix. (2012). ThreatMetrix Report Reveals Fraudulent Transaction Activity on Desktop and Mobile for 2011 Holiday Season. *ThreatMetrix(Online). https://www.threatmetrix.com/press-releases/threatmetrix-report-reveals-fraudulent-transaction-activity-on-desktop-and-mobile-for-2011-holiday-season/*

[38] Federal Trade Commission. (2012). Protecting consumer privacy in an era of rapid change. *FTC report.*

이 보 한(Lee, Bo Han) [정회원]

- 2014년 8월 : 서울대학교 소비자아동학부 소비자학 전공(학사)
- 2014년 8월 : 서울대학교 경영대학 경영학과 전공(학사)
- 2014년 9월 ~ 현재 : 서울대학교 소비자학과 박사수료
- 관심분야 : ICT 환경 속 소비자 행동 및 소비자 정보탐색, 소비자 패널 및 빅데이터를 통한 소비자 후생증진에 관한 연구
- E-Mail : bohan@snu.ac.kr

나 종 연(Rha, Jong Youn) [정회원]

- 1996년 2월 : 서울대학교 소비자아동학부(학사)
- 1998년 2월 : 서울대학교 소비자학과(석사)
- 2002년 5월 : The Ohio State University, Dept. of Consumer and Textile Science(박사)
- 2002년 7월 ~ 2003년 8월 : University of Delaware, Dept. of Consumer Studies, 조교수
- 2004년 8월 ~ 현재 : 서울대학교 소비자학과 교수
- 관심분야 : ICT 소비자정책, 빅데이터 활용과 소비자 프라이버시 보호의 조화, ICT 환경의 변화와 소비자 후생
- E-Mail : jrha@snu.ac.kr