ETRI

2012
Electronics and
Telecommunications
Trends

개인정보 수집 기술 및 대응방안

Survey of the Technologies for Collection of PII

김승현 (S.-H. Kim) 인증기술연구팀 선임연구원
진승헌 (S.-H. Jin) 인증기술연구팀 팀장

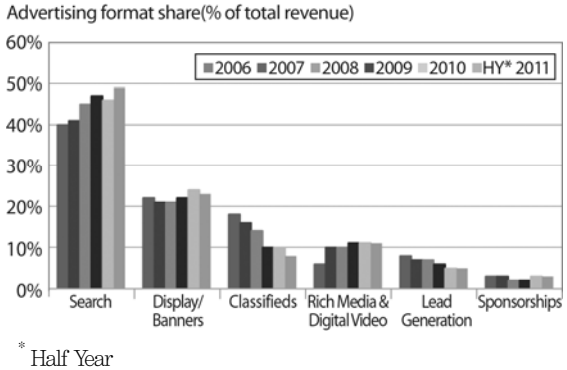
사용자의 동의를 받지 않은 개인정보 수집 기술이 남용되고 있다. 개인정보 수집 업체, 검색엔진 등은 웹브라우징, 스마트폰, 플랫폼 사용 과정에서 개인정보를 수집하여 인터넷 광고, 기업 서비스에 판매하여 수익을 창출한다. 하지만 프라이버시 침해와 관련하여 국내외적으로 개인정보 수집 기술의 문제를 인식하고 대응하려는 분위기이다. 이에 따라 본고에서는 5개의 웹브라우징 개인정보 수집 기술을 설명한다. 그리고 이를 해결하기 위한 근본적인 방안으로 VRM(Vender Relationship Management) 기술을 제안한다.

Ⅰ. 서론

인터넷 광고는 인터넷의 역사와 맥락을 같이한다. 단순한 배너, 텍스트에서 시작하여 최근에는 검색, 소셜 네트워크를 활용한 개인화된 광고에 이르기까지, 인터넷 기술이 발전함에 따라 광고 기술 또한 급격하게 발전하였다. 2011년 상반기의 미국 인터넷 광고 시장은 149억 달러 규모로 작년에 비해 23% 성장한 수치를 보인다[1]. 인터넷 광고 기술은 온라인 IT 기업들이 수익을 얻는 가장 큰 분야로, 특히 Google은 96%, Facebook은 90%의 수익이 광고로부터 나온다[2].

기존의 매스미디어 광고와는 달리, 인터넷 광고는 성과를 비교적 객관적으로 평가할 수 있다. 광고주는 집행된 광고가 더욱 효율적인 성과를 낼 수 있도록 요구하며, 이에 따라 타깃팅된 광고를 요구하는 추세이다. 타깃 광고는 개인의 성향에 기반하여 가장 관심 있을 만한 사람에게 해당 광고를 제시하는 방법으로, 검색엔진을 통한 키워드 검색이나 소셜 네트워크 서비스에서의 개인 성향/대화 내용에 기반한 타깃팅이 가능하다. 현재 일반적인 인터넷 광고 비용은 1,000명당 2달러 수준이나, 타깃 광고는 2배가 넘는 4.1달러에 거래되고 있다[3]. 또한 (그림 1)에서 보듯이, 실제로 검색 기반의 타깃 광고가 매년 성장하는 추세이며 전체 인터넷 광고의 절반을 차지한다[1].

기업 입장에서도 고객을 타깃팅할 필요성이 증대하고 있다. 경제위기에도 불구하고 글로벌 기업과 경쟁해야 하는 상황에서, 대중의 취향을 고려하지 않은 방식으로 여러 가지 서비스를 개발하는 것은 매우 비효율적이며 기업의 존망을 위협하는 안이한 전략이다. 고객의 성향을 기반으로 특정 고객을 타깃팅한 뒤에, 고객이 원하는 서비스를 개발하여 개인화된 경험을 제공해야 한다. 기업은 CRM(Customer Relationship Management)을 통해 고객들의 구매패턴과 다양한 개인정보를 활용하여 맞춤형 서비스를 제공할 수 있었다. 하지만 최근 들어 전 세계적으로 프라이버시에 대한 경각심이 고취되어, 개인정보를 최소한으로 수집하고 정해진 목적으로만 활용해야 하는 법안/규제가 기업을 압박하는 실정이다.



(그림 1) 인터넷 광고 포맷에 따른 점유율 추이

또한 고객정보를 넘어서, 개인의 다양한 성향 정보를 기업 활동에 반영하려는 요구 사항이 존재한다. 하지만 포커스 그룹이나 온라인 여론조사 등의 합법적인 방법보다는, 정보획득의 용이성이나 저비용 이점으로 인해 사용자 동의 없이 수집 가능한 비합법적 기술이 업계의 많은 주목을 받고 있다. 미국 실리콘밸리의 경우 2007년부터 356개의 온라인 광고 벤처에게 47억 달러(약 한화 5조원) 규모의 투자가 이루어졌는데, 이는 고도의 타깃팅된 광고 방식에 대한 수요를 보여준다[4]. 2010년, 미국의 방문자 순위 50위까지의 사이트에서 64개의 추적 기술과 3,180개 파일이 설치되어 충격을 가져왔으며[3], 월스트리트저널은 기획보도[5]로 이 문제를 공론화시켜 기업과 정부의 변화를 이끌어냈다.

본고에서는 웹브라우징 중에 개인의 동의를 받지 않은 채 개인정보를 수집할 수 있는 기술들을 소개한다. 그리고 개인에게 혜택과 프라이버시를 제공하면서, 기업과 업체가 윈-윈 할 수 있는 플랫폼으로 VRM(Vender Relationship Management) 기술을 소개한다.

Ⅱ. 개인정보 수집 기술

1. 개인정보

개인정보는 여러 단체/기관에서 다양하게 정의되어

있다. 이들 정의를 종합하여 개인정보를 한마디로 요약하자면, 개인을 '식별'할 수 있는 모든 정보라고 할 수 있다. 개인정보는 크게 세 가지 종류로 구분되는데, 1) 사용자 본인이 직접 입력한 자발적 정보(예: 이름, 성별, 나이, 주소, 취미), 2) 제3자에 의해 관찰된 정보(예: 웹브라우징 기록, 위치정보), 3) 제3자에 의해 유추된 정보(예: 신용등급, 소비성향 예측)이다.

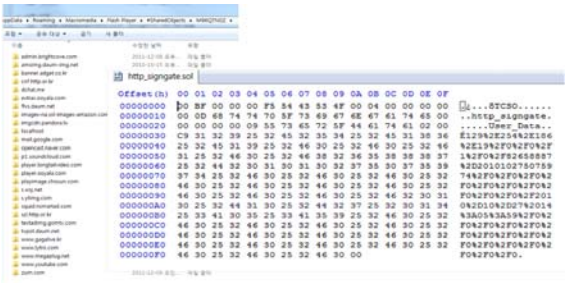
개인정보는 다양한 장치(예: 모바일, PC, 센서)와 소프트웨어(예: 운영체제, 애플리케이션)로부터 생성되며, 서비스 제공자로부터 서비스를 제공받을 때 수집/축적된다. 수집된 개인정보는 다양한 목적으로 활용되며, 최종 사용자/정부 · 공공기관/기업에서 소비된다[6]. 개인정보를 수집하는 '인터넷 추적 회사'와 '인터넷 검색엔진', '모바일 서비스/인터넷 서비스 제공자'들은 서비스/인프라 플랫폼을 기반으로 명시적인 사용자 동의 없이 개인정보를 수집할 수 있으며, 광고 판매와 같은 서비스에 임의로 활용할 수 있기 때문에 주의가 요구된다.

2. 개인정보 수집 기술

가. Cookie & Super Cookie

Cookie는 웹사이트에서 사용자의 로그인 여부나 개인정보를 저장하기 위해 설치하는 몇 바이트 크기의 텍스트 파일이다. Cookie에는 사용자의 식별자가 포함되므로 서비스 제공자는 사용자의 행동을 모니터링할 수 있다. Cookie를 이용한 개인정보 수집은 쉽게 회피할 수 있는데, cookie가 저장되는 디렉토리를 정기적으로 삭제하거나 웹브라우저 자체 또는 플러그인으로 제공되는 cookie 삭제 기능을 활용하면 된다.

Super cookie는 cookie와 마찬가지로 사용자를 모니터링하는 기술이지만, 일반 cookie와는 다른 위치(예: 웹브라우저의 cache 영역, 웹브라우저 플러그인이 설치된 디렉토리)에 저장되기 때문에 일반 사용자는 삭제하기 어렵다. 대표적인 super cookie의 사례로는 Microsoft사의 Media Player Plugin, Adobe사의 Flash, HTML5의 WebStorage 기술이 있는데, 여기서는 Flash 사례를 자세히 살펴보겠다[7].



(그림 2) Flash Cookie의 저장 위치 및 내용

Flash cookie는 보통 Flash 파일을 실행할 때의 사용자 선호 설정을 기억하기 위해 사용된다. 카메라 사용이나 볼륨 조절 같은 경우, 사용자가 한 번만 설정해도 계속 유지된다. 그러나 Flash가 구동된 상태에서 사용자의 활동 내역을 계속 추적할 수 있기 때문에 문제가 된다. 최근에는 비디오 파일, 게임뿐만 아니라 인터랙티브 광고에도 Flash가 자주 사용되기 때문에, 광고에 따른 사용자의 동작 내역이나 페이지 정보 같은 개인정보를 수집 가능하다[8]. Flash cookie는 Flash 플러그인이 실치된 디렉토리에 위치하는데, Microsoft사의 WIN 7인 경우 (그림 2)처럼 'C:₩Users₩{사용자계정}₩AppData₩Roaming₩Macromedia₩FlashPlayer₩#SharedObjects₩{랜덤문자열}'에 Flash cookie가 웹사이트별로 저장된 것을 확인할 수 있다.

나. Beacon

Beacon은 Web Bug라도 불리는 기술로, 일반적으로 1×1 픽셀의 투명한 그림 파일이다. 웹사이트나 이메일의 구석에 위치하며, 웹페이지/이메일이 로드되거나 특정 이벤트가 발생할 때, 사용자의 정보(예: IP 주소, 열람 시간, 브라우저 종류, cookie 존재여부 등)와 행동 내역을 서버에게 전달한다[9]. (그림 3)은 이메일의 버튼을 클릭할 경우, 서버에 이벤트 정보를 저장시키는 beacon

(그림 3) 이메일에 설정된 Beacon 사례

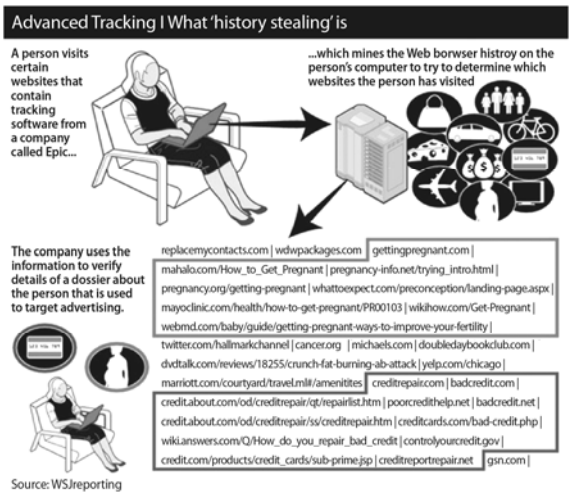
(그림 4) Google Analytic 보고서에서의 방문자 흐름도 화면

을 보인다.

Beacon은 수동적인 관찰 정보밖에 전달하지 못한다는 한계가 있었으나, 최근에는 JavaScript로 작성된 beacon을 통해 다양한 정보를 추출할 수 있다. 일례로 Google사의 Analytics 서비스[10]는 웹사이트를 방문한 사용자의 활동 내역, 시간, 브라우저 타입 등 다양한 정보를 확보할 수 있다. (그림 4)는 Google Analytics의 보고서 샘플 화면을 보인다.

다. History Stealing

History stealing은 사용자의 웹브라우저 접속 기록을 가로채는 기술이다. 일반적으로 웹브라우저는 'a href'로 시작하는 태그를 만나면 해당 웹사이트의 방문 여부에 따라서 링크를 다른 색으로 표시한다. 방문하지 않은 경우는 '파란색', 방문 후는 '보라색'으로 보이기 때문에, 사용자의 해당 웹사이트 방문 여부를 식별 가능하다. History stealing은 바로 웹브라우저의 렌더링 여부를 관찰하여 사용자의 접속 기록을 가로챈다[8].



(그림 5) History Stealing을 이용한 개인정보 수집 사례

구동 절차는 다음과 같다. 먼저, 웹사이트 광고 등을 통해 사용자 웹브라우저에 악성코드가 실행된다. 악성코드는 사용자 모르게 수집할 웹사이트의 링크 목록을 생성하는데, 웹브라우저는 링크 태그를 인식하는 즉시 사용자의 접속 기록에 기반하여 링크 색을 렌더링한다. 악성코드는 해당 링크들의 색을 체크하여 결과를 악성 서버에 전송한다. (그림 5)는 history stealing의 사례를 보여준다. 사용자가 방문한 웹사이트에 Epic이라는 회사의 악성코드가 삽입되어 있는데, 이 악성코드는 수천 개의 링크 목록을 생성하여 사용자가 신용카드와 임신에 관심이 있다는 정보를 확보한다[7].

ActiveX 같은 별도의 플러그인을 설치한다면 아주 쉽게 사용자의 접속 기록을 확보할 수 있겠지만, 웹브라우저에서 확인 가능하며 쉽게 차단할 수 있다. 하지만 history stealing 기술은 별도의 플러그인 설치 없이도 사용자의 접속 기록을 알 수 있으며, 사용자는 침해 여부를 인지하기 어렵다.

라. Fingerprint

Fingerprint는 사용자 장치의 특징을 조합하여 반영구적으로 유일하게 사용자 장치를 식별할 수 있는 기술

〈표 1〉 Fingerprint에 활용되는 브로드캐스트 정보

항목	설명
시간	타임서버와 주기적으로 동기화하지만, 하드웨어/소프트웨어 특성에 따라 시스템별로 수 ms 단위로 차이가 발생함.
폰트	사용자가 별도로 설치한 글자 폰트 목록 차이
화면 크기	웹사이트가 보여지는 화면의 크기, 색상 설정 차이
사용자 ID	한 번 유일하게 식별되면, 추적서버는 시스템에 ID를 부여하여 향후 추적에 활용함.
브라우저 플러그인	사용자가 설치한 웹브라우저의 플러그인 목록
User Agent	시스템 운영체제, 웹브라우저 종류

이다[11],[12]. 사용자 장치는 같은 브랜드 제품/운영체제임에도 불구하고, 시간, 글자 폰트, 설치된 소프트웨어 목록 등의 차이가 존재한다. 〈표 1〉은 웹브라우저가 인터넷에 연결되었을 때 브로드캐스트(broadcast)하는 정보 중에서, fingerprint에 이용되는 정보를 보여준다.

Fingerprint에 사용되는 정보들은 웹브라우징을 하는 도중에 모두에게 공개되기 때문에 누구나 추적 가능하다. Cookie와 유사하지만 더욱 고도의 방법인데, 사용자는 추적되는지 알 수 없으며 파일 삭제와 같은 방법으로도 피할 수 없기 때문이다. 웹브라우저를 업그레이드하거나 플러그인을 설치/삭제하는 식으로 일부 정보를 수정할 경우에도, fingerprint는 다른 여러 특성을 조합한 뒤 사용자 장치의 변경 내역을 인식하여 유일하게 식별 가능하다.

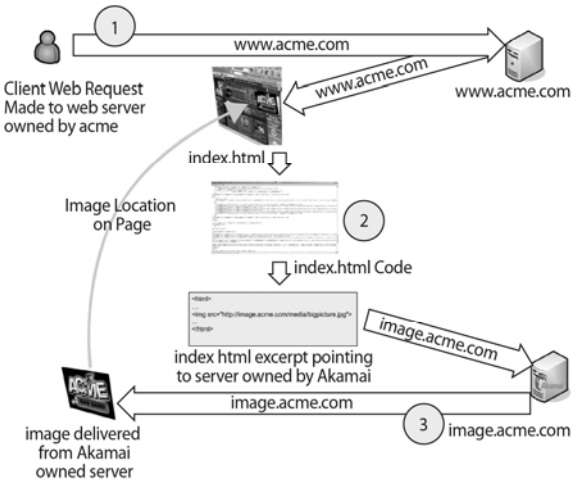
실험 결과에 따르면, fingerprint 기술로 100만 대 중 91%를 유일하게 식별 가능하다고 한다. 실제로 Panopticlick 사이트를 방문하면 본인의 웹브라우저가 유일하게 식별 가능한지 확인할 수 있는데[13], 필자의 경우는 188만 대 중 한 대로 식별 가능하다는 결과가 나왔다. 단순히 웹브라우저의 'User Agent'에 출력되는 운영체제, 웹브라우저 버전/타입, 설치된 플러그인 목록만으로 구분 가능했다. (그림 6)은 필자의 웹브라우저가 fingerprint된 내역을 보인다.

(그림 6) 웹브라우저의 Fingerprint 테스트를 수행하는 사이트 화면

마. Contents Redirection

Beacon은 주로 한 웹사이트에서 이루어지나, 인터넷 레벨에서 콘텐츠 리다이렉션을 통한 개인정보 수집이 가능한 사례가 존재한다.

첫번째는 CDN이다. CDN은 콘텐츠 전송 네트워크(Content Delivery Network)의 약자로, 일종의 캐시 역할을 할 수 있도록 전체 네트워크상에 동일한 콘텐츠 내용을 복제하여 대규모 인트라넷 또는 인터넷상에 분산시켜 놓은 시스템을 말한다. 대표적인 CDN은 인터넷 전체 웹트래픽의 15~30%를 담당하는 미국의 Akamai 사인데, 이 업체는 2008년부터 개인정보 수집 서비스를 제공한다. (그림 7)을 보면 사용자가 특정 웹사이트를 방문할 때 CDN에 저장된 이미지를 가져온다. 이 시점

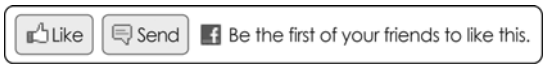


(그림 7) CDN 서비스의 동작 흐름

에서 CDN 서비스는 사용자의 온라인 활동을 쉽게 파악할 수 있다[14].

두번째는 광고서버이다. Cookie는 특정 서버에 국한되어 동작하기 때문에 사용자의 전체적인 온라인 활동 내역이 노출되기 어렵다. 하지만 광고서버의 경우, 사용자가 방문한 웹사이트에 광고가 설치되어 있다면 광고서버 또한 사용자의 활동을 수집할 수 있다. 광고서버는 사용자가 어느 웹사이트의 어떤 페이지에서 광고를 요구하는지를 알 수 있으며, 이에 따라 시간대별로 사용자의 행동과 관심사 등의 정보를 획득 가능하다. 만일 사용자가 특정 광고서버의 광고가 설치된 웹사이트만 방문한다면, 사용자의 전체적인 온라인 활동 내역이 노출되는 것이다.

세번째는 Widget이다. 일반적으로 widget은 Java-Script 형태로 웹페이지에 삽입 가능한데, 소스가 제3의 사이트일 경우 해당 사이트에서 사용자의 활동을 모니터링할 수 있다. 최근 대표적인 사례는 Facebook의 'social widget'이다. Social widget은 Facebook이 아닌 웹사이트의 내용에 '좋아요' 또는 '게시'를 쉽게 퍼갈 수 있는 기능으로 (그림 8)과 같은 모양이다. Social widget을 이용하여 1개월 내에 Facebook에 1번 이상 로그인한 사용자는 추적이 가능하다. 방문순위 상위권 1,000개의 사이트 중, 331개의 사이트가 추적 가능하다. 더욱이 일부 Facebook widget은 cookie를 설정하여, Facebook 홈페이지에 한 번도 방문한 적 없는 사용자의 웹브라우징 데이터를 수집한 바 있다[15].



(그림 8) Facebook의 Social Widget

Ⅲ. VRM

1. 필요성

앞 장에서 소개한 개인정보 수집 기술은 모두 사용자의 개인정보를 명시적인 동의 없이 획득하여 임의로 활용한 사례이다. 실제 사용자와 연결시키지 않았기 때문에 합법적이라고 하지만, 사용자의 프라이버시 침해로 용이하게 연결될 수 있다. 또한 개인정보 수집 기술은 사용자에게 잠재적인 경제적 손실을 초래한다. 사용자는 비록 대부분의 서비스를 무료로 제공받지만, 업체가 개인정보 판매로 벌어들이는 수익은 사용자에게 주어진 금전적인 이익을 가로채는 것과 마찬가지이다.

기업은 자사 내부의 사용자 개인정보와 행동패턴을 파악하여 서비스에 활용할 수 있다. 하지만 법적 규제로 인해, 기업이 수집하는 개인정보는 제한적이며, 이마저도 임의의 목적으로 활용하기 어려워졌다. 기업은 개인 맞춤형 서비스를 제공하여 업계에서의 우위를 유지해야 하기 때문에, 방대한 고객의 성향을 빠르게 확보하기 위해서는 개인정보 수집업체와 협업할 수 밖에 없다. 하지만 업체를 통해 확보한 개인정보로 사용자들의 패턴 파악은 가능하지만, 사용자 행동에 대한 이유를 추측해야 하기 때문에 비효율적이다.

앞으로도 개인정보 수집 시장은 더욱 규모가 커질 전망이다. 하지만 기존의 개인정보 수집 방식은 계속 차단당하고, 고도화된 방식의 추적 기술이 꾸준히 제시될 것이다. 여전히 사용자의 명시적인 동의를 받지 않은 방식인 경우, 방어 기술의 발전으로 인해 사용자 개인정보를 수집하는 비용은 점차 증가하여 투자비용 대비 성과가 저하된다.

이를 해결하기 위해서는 사용자의 명시적인 동의를 기반으로 하는 개인정보 공유 체계가 등장해야 한다. 사용자가 직접 본인의 개인정보를 관리하고, 원하는 서비스 제공자와 공유/판매하는 방식이다. 개인정보 활용 목적과 범위를 명시하여 처리하기 때문에 프라이버시를 보호할 수 있어야 한다. 또한 사용자가 직접 정보를 제공하기 때문에 그에 따른 혜택(돈, 부가 서비스 등)도 직접 받을 수 있어야 한다.

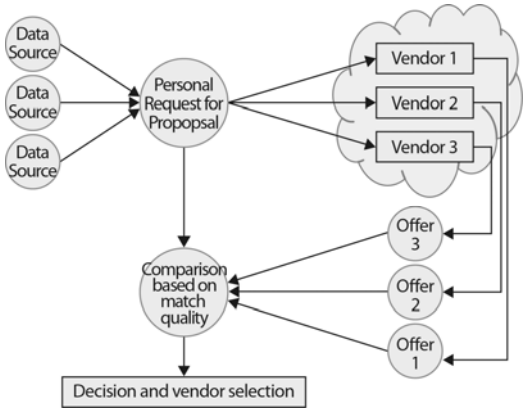
2. VRM

VRM은 Doc Searls이 이끄는 ProjectVRM[16]에서 2006년부터 시작되었으며, 기업이 보관하는 고객 데이터를 고객이 직접 관리한다는 개념에서 시작되었다. VRM은 고객의 관점에서 개인정보를 기업에게 제공하기 위한 다양한 기능을 제공하는데, 〈표 2〉는 그 중에서 주목할 만한 4가지 기능을 소개한다[16].

(그림 9)는 NetMesh의 Johannes Ernst가 작성한 VRM 흐름이다. 우선, 사용자가 개인정보(data source)

〈표 2〉 VRM의 4가지 대표적인 기능

기능	설명
개인용 데이터 저장소	• 사용자의 온/오프라인 활동 기록을 수집, 보관하는 기능(ex. 연락처, 구매, 선호도, 웹서핑, GPS, 일정 등) • 저장된 개인정보를 바탕으로 다른 서비스에 활용할 수 있음
개인용 데이터 분석	• 개인정보를 분석하여 다양한 패턴을 확인 가능 • 분석 결과를 비교하여 고객의 패턴 예측 가능
제안 요청서	• 사용자가 기업에게 제공받고 싶은 서비스 요구사항을 전달하면, 기업은 요구사항을 검토한 뒤 자신들의 제안/가격/약관을 제시하는 역경매 방식의 서비스 • 브로커를 이용한 대행 서비스, 익명 서비스 모델이 존재함.
권한 관리와 역메시징	• 특정 개인정보를 어떤 기업에게 공개할지를 실시간으로 제어함. • 거래 없이도, 기업에게 개인정보를 제공하는 채널을 맺고 혜택을 얻는 서비스



(그림 9) VRM의 동작 흐름

를 활용하여 개인화된 서비스를 요청한다. 제안서(RFP: Request For Proposal)는 사용자의 개인정보를 통해 생성되며, 작성된 제안서는 특정 기업(vender) 또는 불특정 다수 기업이 열람할 수 있다. 기업들이 RFP에 맞는 조건(offer)을 제안하면, 사용자는 본인의 RFP와 비교하여 최선의 서비스를 제공하는 기업을 선택한다. 자세한 구동 방식은 참고문헌 [17]을, 오픈소스로 제공되고 있는 VRM 프로젝트는 참고문헌 [18]을 참조하기 바란다.

VRM은 여러 참여 주체들에게 상호 이익을 줄 수 있는 비즈니스 모델이다. 고객 입장에서, VRM은 고객이 직접 개인정보를 관리하고 필요할 때만 기업에게 제공하므로 프라이버시 문제를 해결한다. 또한 개인정보 제공에 대한 혜택을 사용자가 직접 받을 수 있다. 개인정보를 일원화하여 관리할 뿐만 아니라 데이터를 분석하여 라이프스타일을 제안하는 개인비서와 같은 역할을 VRM 솔루션이 제공할 수 있다.

기업 입장에서, 몇 건의 구매패턴만으로 고객의 성향을 추측해야 하는 CRM과는 달리, VRM은 고객으로부터 직접적인 요구사항과 성향을 수집할 수 있기 때문에 더욱 효과적이다. 또한 고객에게 개인정보 관리를 맡기기 때문에 개인정보 보호와 관련된 법안/규제를 준수하기 위한 비용을 절감할 수 있다.

기존에 개인정보를 은밀히 수집하던 업체들은 VRM 클라이언트와 수집 에이전트를 제공하여 고객과 기업을 연결시키는 채널을 소유할 수 있다. 단순히 개인정보를 판매하는 사업모델에서 벗어나, 개인의 특성을 고려한 맞춤형 광고 등 다양한 서비스를 제공 가능하며 고객의 성향을 파악하고 고객의 구매에 막대한 영향력을 미칠 수 있다.

Ⅳ. 결론 및 향후 방향

본고에서는 사용자 동의 없는 개인정보 수집 기술에 대해 살펴보았다. 인터넷 온라인 광고는 사용자의 성향

에 기반한 타깃 광고가 가능하다는 장점 때문에 각광을 받고 있으며, Google/Facebook 같은 인터넷 기업은 대부분의 수익을 광고로부터 얻는다. 하지만 개인정보에 대한 사용자의 인식이 개선되고 관련 법률의 강화로 인해, 기업이 개인정보를 임의로 확보하기 어려워지고 있다. 이 때문에 개인정보를 은밀히 수집할 수 있는 기술이 주목받고 있다.

본고에서는 웹브라우징 중에 개인의 동의를 받지 않은 채 개인정보를 수집할 수 있는 기술로 cookie, beacon, history stealing, fingerprint, content redirection을 소개하였다. 그리고 개인에게 혜택과 프라이버시를 제공하면서, 기업과 업체가 윈-윈 할 수 있는 플랫폼으로 VRM 기술을 소개했다.

사용자 중심의 개인정보 공유/판매 체계를 수립한다면, 사용자와 기업, 관련 업체가 모두 윈-윈 할 수 있는 환경이 될 것으로 예상한다. 하지만 사용자 동의 없는 개인정보 수집 기술을 차단하지 않으면 VRM의 도입 속도는 매우 느릴 것이다. 따라서 VRM 기술의 개발에는 개인정보 수집 기술을 적극적으로 차단할 수 있는 방안이 필수적으로 요구되어야 한다. 해킹과 보안처럼 창과 방패의 싸움이 지속될 것이나, VRM은 사용자의 권리와 이익에 직접적으로 연관되기 때문에 많은 호응과 자발적인 지원이 예상된다.

용어해설

Cookie 웹사이트가 사용자의 PC에 저장해 둔 텍스트 파일로, 사용자의 개인정보나 로그인 등 활동 내역 등의 정보를 관리/활용하기 위한 목적을 가짐.

타깃 광고 개인정보 또는 활동 성향에 기반하여 가장 관심 있을 만한 사람에게 해당 광고를 제시하는 방법으로, 검색엔진의 키워드 광고, SNS(소셜 네트워킹 서비스)에서의 광고가 대표적임.

약어 정리

CDN	Content Delivery Network
CRM	Customer Relationship Management
HTML	Hyper Text Markup Language
PII	Personal Identifiable Information
RFP	Request For Proposal
VRM	Vender Relationship Management

참고문헌

[1] IAB, "IAB Internet Advertising Revenue Report, 2011 First Six Months Results," Sept. 2011. www.iab.net/media/file/IAB-presentation-HY2011_FINAL.pdf

[2] Bloomberg, "Facebook Revenue Will Reach $4.27 Billion, EMarketer Says," Sept. 21th, 2011.

[3] Wall Street Journal, "The Web's New Gold Mine: Your Secrets," July 30th, 2010.

[4] Wall Street Journal, "Online Trackers Rake In Funding," Feb. 24th, 2011.

[5] Wall Street Journal, "What They Know,". http://online.wsj.com/public/page/what-they-know-digital-privacy.html

[6] World Economic Forum, "Personal Data: The Emergence of a New Asset Class," Jan. 2011.

[7] Wall Street Journal, "Latest in Web Tracking: Stealthy 'Supercookies'," 19th Aug. 2011.

[8] Wall Street Journal, "Suit to Snuff Out 'History Sniffing' Takes Aim at Tracking Web Users," Dec. 5th, 2010.

[9] http://www.allaboutcookies.org/web-beacons/

[10] http://www.google.com/analytics/

[11] Wall Street Journal, "Race Is On to 'Fingerprint' Phones," PCs', Nov. 30th, 2010.

[12] Wall Street Journal, "How To Prevent Device Fingerprinting," Nov. 30th, 2010.

[13] http://panopticlick.eff.org/

[14] Wall Street Journal, "A New Type of Tracking: Akamai's 'Pixel-Free' Technology," Nov. 30th, 2010.

[15] Wall Street Journal, "'Like' Button Follows Web Users," May 18th, 2011.

[16] http://blogs.law.harvard.edu/vrm/

[17] 김승현, 진승헌, "VRM: 사용자 중심의 고객관계관리(CRM)," 주간기술동향, vol. 1480, 2011, 1. pp. 1-12.

[18] 김승현, 김석현, 진승헌, "VRM 관련 오픈소스 프로젝트 동향," 정보보호학회지, vol. 21, no. 4, 2011. 6, pp. 47-56.