

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-018-243호 (사건번호 : 2024조일0042)

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 Meta Platforms, Inc.

대표자

의결연월일 2024. 11. 4.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

가. 이용자의 페이스북 활동 등을 통해 민감한 주제에 해당하는 광고 타겟을 생성하는 경우 이용자에게 법정 고지사항을 알린 후 별도 동의를 받는 등 보호법 제23조에 따른 적법 근거를 마련하고, 안전성 확보 조치를 취할 것

나. 이용자의 개인정보 열람 요구가 있는 경우 성실히 응할 것. 이를 위해 개인정보 제공 현황 등을 일정 기간 보관하거나, 이용자가 그 현황을 쉽게 확인·통제할 수 있도록 조치할 것

다. 처분통지를 받은 날로부터 90일 이내에 시정명령 이행 계획을 개인정보보호 위원회에 제출할 것

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 21,613,000,000원

나. 과 태 료 : 10,200,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간
공표한다.

이 유

I. 기초 사실

피심인은 페이스북 및 인스타그램 등 서비스를 한국 이용자에게 제공하면서 그 개인정보를 처리하고 있는 「舊 개인정보 보호법¹⁾」(이하 '舊 보호법')에 따른 개인정보처리자이며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 제2조 제1항 제3호에 따른 정보통신서비스 제공자로서 일반현황과 매출액은 다음과 같다.

<피심인 일반현황>

CEO	설립일자	종업원 수	자본금	전체 매출액('21)
주소				

<피심인 매출액 현황>

(단위 : 백만\$)

구분	2019년	2020년	2021년
광고 매출액			
기타 수입			
전체 매출액			

피심인은 2018년 7월 14일부터 페이스북 및 인스타그램 서비스를 대한민국에서 제공하였고, 2021년 9월 기준으로 페이스북 및 인스타그램 서비스의 월간 활성 한국 이용자 계정 수는 각각 개와 개²⁾이다.

1) 舊 개인정보 보호법(2023. 3. 14. 법률 제19234호로 개정되기 전의 것)

2) 2021년 9월 30일 기준 관련 제품의 월간 활성 한국 이용자 수를 제출

2019년부터 2021년까지 페이스북 및 인스타그램 서비스의 연도별 전체 월간 활성 이용자 중 한국 이용자 비율은 아래와 같다.

<피심인 서비스 한국 이용자 비율>

구분	2019년	2020년	2021년
페이스북			
인스타그램			

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회(이하 ‘위원회’)는 피심인의 개인정보 무단 수집·제공 등 다수 조사·처분 과정에서 동의 없는 민감정보 처리, 피심인이 개인정보 열람을 거부하였다는 민원 및 해킹 등을 통해 개인정보가 유출되었다는 신고 등이 접수되어 해당 사건과 관련한 피심인의 개인정보 처리실태를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 동의 없는 민감정보 처리 관련

1) “종교관 및 정치관” 수집

피심인은 2021년 7월까지 페이스북 프로필의 “기본 정보”란을 통해 이용자의 종교관 및 정치관 등 민감정보를 입력받아 수집하였으며, 종교관 또는 정치관 정보를 입력한 한국 활성 이용자는 명³⁾으로 확인된다.

3) 전 세계 활성 이용자는 명, 2021년 3월 26일부터 2021년 4월 24일 기준

< 페이스북 프로필 수집 화면 >



피심인은 페이스북 프로필의 종교관 및 정치관의 경우 이용자가 자신이 원하는 정보를 맞춤화하고 설정에 따라 공유할 수 있도록 하는 등의 목적으로 사용되고, ‘광고 타겟팅’ 등에는 사용하지 않는다고 소명⁴⁾하였다.

피심인은 2021년 8월, 조사 과정에서 한국 이용자의 경우 페이스북 프로필에 종교관 및 정치관을 입력할 수 없도록 필드를 삭제하였고, 수집된 정보를 자진 파기하였다.

2) “동성과 결혼” 정보 수집·이용

피심인은 페이스북 프로필의 “결혼/연애 상태”를 통해 2021년 12월 16일 기준 한국 월간 활성 이용자 명의 “동성과 결혼” 여부 정보를 수집하였다.

< 페이스북의 “결혼/연애 상태” 정보를 수집하는 화면 >



4) 반면, 메타의 데이터 정책에는 “특별 보호를 받는 정보”(종교관, 정치관, “관심 있는” 사람 또는 건강 정보)를 맞춤화된 Facebook 제품을 만들기 위해 이용하고, 광고 및 기타 홍보 콘텐츠에 이용한다고 공개되어 있음

피심인은 광고주가 이용자 프로필 정보의 “결혼/연애 상태”를 타겟으로 광고할 수 있도록 하였고, 2014년 이후 “결혼/연애 상태”가 “동성과 결혼”인 이용자를 타겟으로 광고를 게재한 광고주는 2021년 12월 16일 기준으로 총 개로 확인되며, 이용자가 “결혼/연애 상태”의 공개 범위를 비공개(“나만 보기”)하더라도 광고가 게재될 수 있었다.⁵⁾

< 정보 수집 및 광고 타겟팅 화면 >

피심인은 한국 이용자가 프로필에 “동성과 결혼” 여부를 입력할 수 있도록 의도한 것이 아니고, “in a civil union(시민 결합 상태)”을 번역하는 과정에서 오역되었다고 소명하였으며, 2022년 3월에 이를 “시민 결합”으로 수정하였다.

< “동성과 결혼” 관련 피심인의 답변(2022년 1월 28일 답변 발체) >

5) “결혼/연애 상태”를 비공개(“나만 보기”)하더라도 광고가 게재될 수 있으며, 광고 타겟팅 대상에서 제외하려면 광고 기본 설정 (계정→설정 및 개인정보→계정 센터→광고 기본 설정→회원님에게 도달하기 위해 사용된 카테고리)에서 제외하여야 함

3) 민감정보 관련 광고 타겟 운영·제공

피심인은 이용자가 '좋아요'를 누른 페이지, 클릭한 광고 등을 분석하여 광고주에게 광고 타겟으로 제공되는 특정 광고 주제에 해당하는 경우, 이용자와 특정 광고 주제를 연결하여 분류·관리⁶⁾하였다.

피심인이 생성·운영한 광고 주제는 2021년 3월 3일 기준으로 총 개이며, 해당 광고 주제에는 불교·힌두교·감리교·여호와와 증인·북한이탈주민, 동성애·트랜스젠더 등이 포함되어 있었다.

< 이용자 계정에 연계된 광고 주제 >



특정 광고 주제와 연계된 페이스북 이용자 수는 아래와 같다.

< 일부 광고 주제별 이용자 수(2021년 12월 16일 기준) >

광고 주제	적용시점	예상 타겟 규모	
		전 세계 이용자	한국 이용자
불교	'11년~	219,514,617~258,149,190	601,200~707,300
힌두교	'11년~	222,531,921~261,697,540	205,400~241,600
감리교	'11년~	9,437,704~11,098,740	34,800~41,000
동성애	'11년~	37,726,003~44,365,780	438,600~516,000
트랜스젠더	'11년~	28,865,017~33,945,260	55,900~65,700
북한이탈주민	'11년~	140,093~164,750	9,800~11,600

6) 광고 기본 설정(계정→설정 및 개인정보→설정→계정 센터→광고 기본 설정→광고 주제)에서 이용자에게 태그된 광고 주제 확인 가능

피심인은 광고주가 특정 광고 주제가 연결된 이용자를 대상으로 광고를 게재할 수 있도록 광고 주제 전체를 광고 타겟으로 제공하였으며, 광고주는 페이스북 및 인스타그램 등에서 사상·신념, 성생활 등 민감정보에 해당하는 광고 주제를 타겟으로 광고를 게재한 사실이 있다.

< 광고 관리자의 상세 타겟팅 화면 >

상세 타겟팅

일지하는 사람 포함 ⓘ

인구 통계학적 특성

관심사

행동

가족 및 결혼/연애 상태

비즈니스 및 산업

쇼핑 및 패션

스포츠 및 야외활동

식품 및 음료

엔터테인먼트(사회적 개념)

엔터테인먼트(사회적 개념)

TV(영화/TV)

게임(재미)

독서(커뮤니케이션)

라이브 이벤트

극장(공연 예술)

나이트 클럽(박, 클럽, 밤 문화)

상세 타겟팅

일지하는 사람 포함 ⓘ

관심사 > 기타 관심사

동성애

인구 통계학적 특성, 관심사 또는 행동 추가

추천 찾아보기

제외

타겟 좁히기

일일 추산 결과

규모: 44,365,780

관심사 > 기타 관심사 > 동성애

설명: 동성애에 대한 관심을 표현했거나 관련 페이지를 좋아하는 사람들

< 민감정보에 해당하는 광고 주제를 타겟으로 게재된 광고 >

--	--

피심인은 민감정보 관련 오해의 소지가 있는 광고 주제는 사람이 검토하고 새로운 광고 주제가 추가되는 경우 사전 검토 및 승인 절차가 있으나, 광고 주제 관리(생성·대분류·소분류·삭제 등)를 위한 매뉴얼은 없고, 종교, 북한이탈주민, 동성애·트랜스젠더 등이 배제되지 않은 이유는 확인 불가능하다고 답변하였다.

피심인은 광고주들이 광고 게재 시 특정 광고 주제(인종, 민족, 성적 지향 및 종교 등)를 가진 이용자를 배제하는 것을 허용하지 않으며, 종교·성적 지향 등 개인적 특성을 이유로 차별하거나 차별을 조장하면 안 된다는 내용의 광고 정책 준수 여부를 확인하였다고 소명하였다.

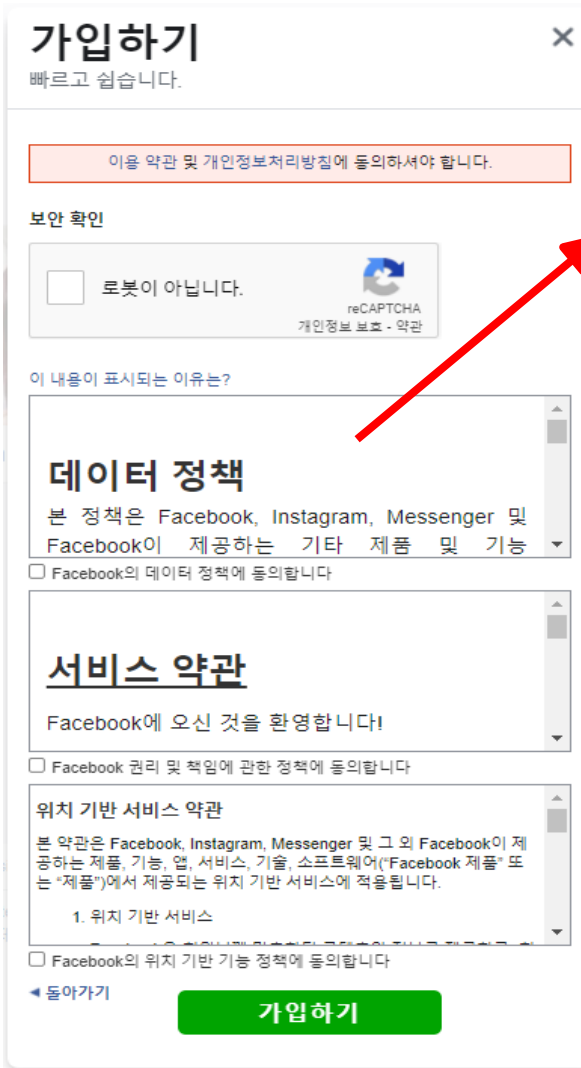

< 광고 주제 항목 배제 관련 피심인의 답변(2021년 8월 29일 답변 발췌) >

피심인은 2022년 1월 19일 민감정보에 해당하는 광고 주제를 광고 옵션에서 제거하기 시작하였고, 2022년 3월부터 광고주가 더 이상 해당 광고 주제를 상세 타겟팅하여 맞춤형 광고를 게재할 수 없도록 조치하였다.

4) 민감정보 처리에 대한 이용자 동의

피심인은 이용자가 서비스 가입 시 데이터 정책에 동의하였다고 답변할 뿐, 민감정보 처리와 관련한 별도 동의를 받은 자료는 제출하지 않았고, 페이스북 서비스에서 민감정보 처리 관련 별도의 동의를 받는 화면은 확인되지 않는다.

< 피싱인이 제출한 데이터 정책 동의 >

 <p>가입하기 빠르고 쉽습니다.</p> <p>이름 약관 및 개인정보처리방침에 동의하셔야 합니다.</p> <p>보안 확인</p> <p><input type="checkbox"/> 로봇이 아닙니다.  reCAPTCHA 개인정보 보호 - 약관</p> <p>이 내용이 표시되는 이유는?</p> <p>데이터 정책 본 정책은 Facebook, Instagram, Messenger 및 Facebook이 제공하는 기타 제품 및 기능</p> <p><input type="checkbox"/> Facebook의 데이터 정책에 동의합니다</p> <p>서비스 약관 Facebook에 오신 것을 환영합니다!</p> <p><input type="checkbox"/> Facebook 권리 및 책임에 관한 정책에 동의합니다</p> <p>위치 기반 서비스 약관 본 약관은 Facebook, Instagram, Messenger 및 그 외 Facebook이 제공하는 제품, 기능, 앱, 서비스, 기술, 소프트웨어("Facebook 제품" 또는 "제품")에서 제공되는 위치 기반 서비스에 적용됩니다.</p> <p>1. 위치 기반 서비스</p> <p><input type="checkbox"/> Facebook의 위치 기반 기능 정책에 동의합니다</p> <p>돌아가기 가입하기</p>	<p>Facebook이 수집하는 정보의 유형 (...) 회원님 및 다른 사람들의 활동 및 제공하는 정보. "Facebook 이 수집하는 정보의 유형"</p> <ul style="list-style-type: none"> • 회원님이 제공하는 정보 및 콘텐츠. (...) • 특별 보호를 받는 정보: Facebook 프로필 필드 또는 중요 이벤트에 <u>회원님의 종교관, 정치관, "관심 있는" 사람 또는 건강 정보를 제공하도록 선택할 수 있습니다. 이러한 정보 및 기타 정보(예를 들어 인증 또는 민족적 태생, 철학적 신념 또는 노동조합 가입 여부)는 회원님의 해당 국가 법률에 따라 특별 보호를 받을 수 있습니다. (...)</u> <p>Facebook이 정보를 활용하는 방법 (...) Facebook 제품의 제공, 맞춤화 및 개선. (...) Meta 제품을 제공하는 데는 <u>기능 및 콘텐츠(귀사 광고, Facebook 뉴스피드, Instagram 피드 및 Instagram 스토리 포함)를 맞춤화하고 Meta 제품 안팎에서 회원님이 관심을 가질 만한 그룹 또는 이벤트나 팔로우할 만한 주제 등을 추천하는 것이 포함됩니다. 회원님을 위해 특별하고 관련성 있는 맞춤화된 Meta 제품을 만들기 위해, 저희는 수집한 데이터와 회원님 및 다른 사람으로부터 얻은 정보(회원님이 제공하기로 선택한 특별 보호 데이터 포함)에 기초한 회원님의 관계, 기호, 관심사 및 활동, 회원님이 Meta 제품을 이용하고 상호 작용하는 방법, Meta 제품 안팎에서 회원님과 연결되어 있거나 회원님이 관심 있는 사람, 장소 또는 사물에 관한 정보를 이용합니다. (...)</u></p> <p>측정, 분석 및 기타 비즈니스 서비스 제공. (...)</p>
---	--

또한, 피싱인이 이용자의 "동성과 결혼" 정보를 수집하고, 페이스북 활동 분석을 통해 이용자와 민감정보에 해당하는 광고 주제를 연결 및 분류·관리하여 광고주에게 광고 타겟 제공 및 광고 게재 목적으로 사용한 것에 대한 별도의 동의 절차도 확인되지 않는다.

나. 개인정보 열람 관련

피심인은 2021년 5월 17일 접수된 신고인⁷⁾의 개인정보 열람 요구에 대해 2021년 5월 18일 신고인에게 열람청구 방법을 안내하였고, 2021년 6월 1일 접수된 개인정보 열람 요구에 대해 2021년 6월 8일 검토 중을 사유로 열람 연기 후 2021년 6월 22일 최종 답변하였다.

피심인은 신고인의 7개 열람 요구 중 2개 사항(질의 2, 3)에 대해서는 열람 요구에 응하였으며, 5개 사항(질의 1, 4, 5, 6, 7)은 보호법에 따른 열람 요구 범위가 아니라면서 일부 사항에 대해서는 아래와 같이 답변을 제공하였다.

< 신고서에 첨부된 열람 요구 및 피심인 답변 >

질의	열람 요구	피심인 답변
1		
2		
3		
4		
5		

7) 신고인은 피심인으로부터 개인정보 열람 요구에 대해 기한 내 답변받지 못했고, 그 답변도 열람 요구 관련 답변이 아닌 열람을 회피하는 회신을 받았다고 민원 제기(국민신문고, 2021년 8월 24일)

6		
7		

피심인은 열람 거절 사유와 관련한 위원회의 자료 요구에 대해 신고인의 열람 요구는 열람 요구권의 범위에 속하지 않는다면 아래와 같이 답변하였고, 신고인에게는 이를 충분히 설명하면서도 일부 열람 요구에 대해서는 답변하였으며, 페이스북 로그인을 통한 정보 공유의 성격(제3자 제공 해당 여부)은 위원회와 소송 중인 사안임을 소명하였다.

< 피심인의 열람 거절 사유 >

질의	열람 요구	거절 사유
4		
5		
6		
7		

피심인은 자료 보유 여부와 관련한 위원회의 자료 요구에 대해 ‘이용자가 페이스북 로그인을 통해 사용한 제3자 앱에 제공된 개인정보’ 및 ‘페이스북 친구가 제3자 앱을 사용하는 과정에서 제3자 앱이 접근 가능하였던 개인정보’와 관련한 자료는 대부분 보유하고 있지 않다고 아래와 같이 답변하였다.

< 피심인이 보유하고 있는 자료 >

구분	보유 여부	비고
• 이용자의 가입일 정보	○	• 개인정보 설정에서 가입일 열람 가능
• 페이스북 로그인을 통해 사용한 제3자 앱에 제공된 개인정보		
- 제3자 앱 이름	△	• 전체 기간에 대한 자료는 없으며, 이용자가 페이스북 로그인을 통해 로그인한 웹·앱 목록은 '내 정보 확인하기' 등을 통해 확인 가능 ※ 이용자가 앱 및 웹사이트 활동과 연결 해제 시 해당 기록은 포함되지 않을 수 있음
- 제공된 개인정보 항목	△	• '20년 2월 16일부터 보유하고 있음
- 제3자 앱 설치·사용 일시	△	• 해당 앱과 관련된 가장 최근 기록을 보유함
- 친구 개인정보에 제3자 앱의 접근 가능 여부 및 항목	X	• 제3자 앱에 제공된 개인정보 항목은 '20년 2월 16일부터 보유하고 있는데, 이는 친구 정보를 제3자 앱과 공유 금지 후 수년이 경과한 시점임
- 제3자 앱이 접근한 이용자의 페이스북 친구 목록	X	
• 페이스북 친구의 제3자 앱 사용으로 인해 제3자 앱에 제공된 개인정보		
- 제3자 앱 이름	X	• 이용자의 개인정보 설정 및 앱에 부여된 권한에 대한 현재 기록은 보유하고 있으나, - 페이스북 이용자 및 친구의 과거 개인정보 설정 기록 또는 앱에 부여한 권한에 대한 기록은 보유하고 있지 않음
- 제3자 앱을 사용한 페이스북 친구 목록	X	
- 제공된 개인정보 항목	X	
- 페이스북 친구가 제3자 앱을 설치·사용한 일시	X	

다. 개인정보 유출 관련

1) 타임라인 미리보기 사건

신원 미상의 자(이하 '해커')는 피심인이 운영하는 페이스북 서비스의 타임라인 미리보기 기능⁸⁾에 존재하는 버그⁹⁾를 악용하여 페이스북 이용자 계정 약 3천만

8) 자신이 타임라인에 작성한 게시물 등이 다른 사람에게 어떻게 보이는지 미리 확인하는 기능

9) 페이스북 서비스의 타임라인 미리보기 기능에는 이용자의 생일이 타임라인에 나타날 때 '미리보기' 모드로 페이지를 열람하면 '쓰기 기능'이 있는 '생일 축하 게시물 게시 도구'가 생일 이벤트와 함께 나타나는데, '생일 축하 게시물 게시 도구'에 포함된 '동영상 업로드'에는 '미리보기'의 대상인 이용자(페이스북 친구 등)의 개인정보를 얻는 데 사용될 수 있는 API 접근권한이 있는 액세스 토큰이 포함되어 있었음(2017년 7월 12일 도입된 버전의 '동영상 업로드'에서 발생)

개의 액세스 토큰을 탈취하여 한국 페이스북 이용자 계정 34,891개의 성명, 이메일 주소, 전화번호, 특정 프로필 정보 등 개인정보를 유출하였다.

<유출 항목 및 계정 수>

유출항목	유출 이용자 계정 수	
	전 세계	한국
• 기본 정보(성명, 이메일 주소, 전화번호)		
• 기본 정보 + 특정 프로필 정보* * 성별, 지역, 결혼 상태, 종교, 출신지, 생년월일 등		
• 기본 정보 + 특정 프로필 정보 + 추가정보** ** 타임라인 게시물, 친구 목록, 소속 그룹, 최근 메시지 대화명		
• 합계		34,891개

< 해커의 타임라인 미리보기 버그를 통한 개인정보 유출 상세 >

- ① 이용자 계정의 친구 ID 목록, 이용자 생일이 타임라인 상단에 위치하도록 타임라인에서 숨겨야 할 포스팅 개수, 이용자 계정의 액세스 토큰 파악
- ② 이용자 액세스 토큰을 쿠키로 변경하여 계정의 프로필을 웹 브라우저에 로딩
- ③ (가능한 경우*) 이용자 계정에서 이용자 생일 이후 포스팅을 타임라인에 숨겨서("Graph API 명령" 사용) 생일 관련 내용이 타임라인 상단에 위치하도록 한 후, '미리보기' 모드에서 생일축하 게시물 게시 도구가 상단에 나타나도록 함
* 이용자가 이미 3명 이상으로부터 생일 축하 메시지를 받은 경우에만 가능
- ④ 이용자 계정의 '미리보기' 모드를 친구 관점(순차적으로 변경)에서 열람한 후, 생일축하 게시물 게시 도구가 있는 경우, 해당 친구 ID에 해당하는 액세스 토큰 수집
- ⑤ ④에서 수집한 액세스 토큰을 이용하여 Graph API를 통해 개인정보 탈취
- ⑥ ④에서 수집한 액세스 토큰 하나를 다시 이용자 계정으로 두고 기존 과정 반복

피싱인은 자체 운영 중인 탐지시스템을 통해 개별 이용자의 로그인 패턴 분석 및 로그인 시도의 유효성 여부를 추론하고 있었으며, 비활성 이용자 트래픽의 급격한 증가를 확인하고 이를 조사하는 과정에서 유출을 인지, 수사 의뢰 및 취약점 조치 등을 수행한 사실이 있다.

일시	유출 인지 및 대응 내용
'18. 9. 17.	• '18. 9. 14.에 시작된 비활성 이용자 트래픽의 급격한 증가를 확인
'18. 9. 25.	• 트래픽의 급격한 증가가 악의적인 활동의 결과라는 것을 확인
'18. 9. 26.	• 미국 연방수사국(FBI) 신고
'18. 9. 27. ~ '18. 9. 28.	• 타임라인 미리보기 버그에 대한 취약점 패치 • 일시적으로 타임라인 미리보기 기능 중단 • 영향을 받았다고 파악된 계정(약 개)의 액세스 토큰 무효화
'18. 9. 28.	• 영향을 받은 한국 이용자(언어:영어)에게 영어로 메시지 발송
'18. 10. 1.	• 영향을 받은 한국 이용자(언어:한국어)에게 한국어로 메시지 발송

또한, 피심인은 버그가 발생한 ‘생일 축하 게시물 도구’의 동영상 업로드 기능은 배포하기 전 ①코드를 작성하지 않은 엔지니어가 검토하고, ②보안 리스크 자동 코드 검토(발견 시 전문 엔지니어 검토), ③구문오류 탐지, 코드 원칙 준수, 사생활 보호 및 보안 문제 확인 관련 자동 테스트 및 ④직원 베타 테스트를 진행하였으며, 소규모 이용자 배포 후 전체 배포를 진행하였다고 소명하였다.

2) 신분증 도용 사건

신원 미상의 자(이하 ‘해커’)는 특정 이용자의 신분증을 위조(도용)하여 피심인이 사용하지 않는¹⁰⁾ ‘과거 계정 복구 양식’을 통해 2020년 8월 4일부터 2020년 9월 5일 까지 페이스북 계정 비밀번호에 대한 재설정 요청을 하였고, 피심인이 이를 승인 하여 해커는 해당 이용자의 페이스북에 로그인 및 개인정보를 유출할 수 있었다.

< 해커가 이용한 ‘과거 계정 복구 양식’ URL >

10) 2020년 5월 28일과 2020년 8월 18일 사이에 단계적으로 사용 중단 절차를 진행함

이로 인해 전 세계적으로 개, 한국의 경우 10개의 페이스북 계정에 대해 권한 없는 접근이 이루어질 수 있었고, 페이스북에 로그인하면 해당 계정의 프로필 등 개인정보를 유출할 수 있다.

< 신분증 도용 관련 개인정보 유출 상세 >

- ① 해커는 특정 이용자의 계정을 선택
- ② 페이스북 로그인 페이지에서 “비밀번호를 잊으셨나요? 버튼 클릭
- ③ 해당 계정과 연관된 이메일 주소 또는 이름 입력
- ④ 해커는 브라우저 검색창에 특정 URL을 입력하여 과거 계정 복구 양식 활성화 및 위조된 신분증 및 새로운 이메일 주소 업로드
- ⑤ 해당 신분증이 인적 오류로 승인, 새로운 이메일 주소로 비밀번호 재설정 링크 발송
- ⑥ 해커는 새로운 이메일 주소와 비밀번호를 사용하여 계정에 로그인

피심인은 신분증 제출 급증 및 미검증 기기의 신분증 제출을 확인하여 공격을 인지하여 문제점 개선 등 조치하고, 영향을 받은 이용자 계정에 대해 추가적인 활동을 할 수 없도록 ‘해킹 잠금(hacked-lock)’ 처리하였다.

일시	유출 인지 및 대응 내용
'20. 8. 4.	• 해커의 공격 시작
'20. 8. 10.	• 추가 계정 복구 도구를 통한 신분증(ID) 제출이 급증한 사실 확인 ※ 피심인의 검토 시스템은 신분증 승인을 거절함
'20. 8. 18.	• 신분증이 ‘ 미검증 기기 ’를 통해 제출되고 있음을 확인
'20. 8. 26.	• 주요 계정 복구 양식에 대한 패치 작업 수행 ※ 추가 계정 복구 과정의 검증단계를 적절히 적용하기 위함
'20. 8. 28. ~ '20. 9. 5.	• 한국 이용자 계정이 영향 을 받음 • 과거에 제공한 계정 복구 양식(4개) 삭제
'20. 9. 7.	• 모든 개선 조치 완료
'20. 9. 11.	• 한국 이용자들이 영향을 받은 사실을 확인 • 개인정보 유출 신고

또한, 해커가 계정에 접근하기 위해 추가한 정보(예 : 이메일 주소, 전화번호)는 삭제하였으며, 재발 방지를 위해 사용하지 않는 비밀번호 재설정 양식은 모두 제거하고, 계정 복구 요청에 대한 지속 모니터링 및 새로운 신분증 검증 절차를 추가하였다.

피심인은 사용하지 않는 과거 계정 복구 절차에 사용된 양식을 페이스북 사이트에서 접근할 수 없도록 조치¹¹⁾하고 신규 양식으로 대체하였으나, 과거 계정 복구 양식 페이지 자체를 완전히 삭제하지 않아 URL을 직접 입력하는 경우 접근이 가능하였다.

그리고 이를 통해 신분증이 제출되는 경우, 피심인은 계정을 복구하려는 자가 검증된 기기를 사용하는지 여부, 과거 페이스북 사용에 연관된 동일한 범위의 IP주소를 사용하는지 여부 등을 검증하지 않고 비밀번호를 재설정 한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2024년 9월 13일 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2024년 10월 4일에 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 관련 법규 및 위법성 판단

1. 관련법 규정

가. 舊 보호법 제23조제1항은 “개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다”고 규정하면서 “정보주체에게 제15조제2항 각 호 또는 제17조 제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를

11) 및 페이스북 경로에서 접근할 수 없도록 조치

받은 경우^(제1호)” 및 “법령에서 민감정보의 처리를 요구하거나 허용하는 경우^(제2호)” 민감정보의 처리가 가능하다고 규정하고 있다.

나. 舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

같은 법 시행령¹²⁾(이하 ‘舊 시행령’) 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다”고 규정하고 있으며, 제2호는 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치’를 하여야 한다고 규정하고 있다.

또한 舊 개인정보의 기술적·관리적 보호조치 기준¹³⁾(이하 ‘舊 고시’) 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유 설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다”고 규정하고 있다.

다. 舊 보호법 제35조제3항은 “개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다”고 규정하면서, 제4항에서 “법률에 따라 열람이 금지되거나 제한되는 경우^(제1호)”, “다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우^(제2호)”에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다고 규정하고 있다.

12) 개인정보 보호법 시행령(대통령령 제34309호, 2024. 3. 12. 일부개정, 2024. 3. 15. 시행)

13) 개인정보의 기술적·관리적 보호조치 기준(개인정보보호위원회 고시 제2020-5호, 2020.8.11. 제정)

舊 시행령 제41조제1항은 “정보주체는 법 제35조제1항에 따라 자신의 개인정보에 대한 열람을 요구하려면 개인정보의 항목 및 내용^(제1호), 개인정보의 수집·이용의 목적^(제2호), 개인정보 보유 및 이용 기간^(제3호), 개인정보의 제3자 제공 현황^(제4호), 개인정보 처리에 동의한 사실 및 내용^(제5호) 중 열람하려는 사항을 개인정보 처리자가 마련한 방법과 절차에 따라 요구하여야 한다”고 규정하면서, 제4항은 “법 제35조제3항 전단에서 ‘대통령령으로 정하는 기간’이란 10일”이라고 규정하고 있다.

2. 위법성 판단

가. 적법 근거 없이 민감정보를 처리한 행위

[舊 보호법 제23조(민감정보 처리 제한)제1항]

피심인이 페이스북 “프로필”을 통해 수집·이용한 이용자의 “종교관” 및 “정치관”과 “동성과의 결혼” 여부는 명백히 보호법 문언상 민감정보에 해당한다.

또한, 피심인이 이용자가 “좋아요”를 누른 페이지, 클릭한 광고 등 활동 분석을 통해 이용자 계정과 연계된 광고 타겟 중 이용자에 관한 사상·신념, 성생활 등에 해당하는 민감한 광고 주제¹⁴⁾도 특정 이용자에 관한 정보¹⁵⁾로서 보호법상 민감정보에 해당한다.

참고로 온라인 맞춤형 광고 개인정보보호 가이드라인(2017.2.)은 “이용자 동의 없이는 행태정보를 이용·분석하여 정보통신망법 제23조제1항에 따른 민감정보를 수집·생성 활용하여서는 아니된다.”라고 안내하고 있다.

피심인은 “동성과의 결혼” 여부와 “이용자 계정과 연계된 민감정보에 해당하는 광고 주제”를 광고 타겟으로 제공하여 광고주의 광고 게재에 활용되도록 하였는데 이는 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에 해당하지 않는다.

14) 불교, 힌두교, 감리교, 여호와의 증인, 북한이탈주민, 동성애, 트랜스젠더 등

15) 정보주체와 관련되어 있으면 키, 나이, 몸무게 등 ‘객관적 사실’에 관한 정보나 그 사람에 대한 제3자의 의견 등 ‘주관적 평가’ 정보 모두 개인정보가 될 수 있다. 또한, 그 정보가 반드시 ‘사실’이거나 ‘증명된 것’이 아닌 부정확한 정보 또는 허위의 정보라도 특정한 개인에 관한 정보이면 개인정보가 될 수 있다.(개인정보 보호 법령 및 지침고시 해설, 2020.12., 제11면)

따라서 피심인이 이러한 정보들을 이용자로부터 수집하거나, 이용자를 연결 및 분류·관리하여 맞춤 서비스·광고 등에 활용하는 등 처리하면서 이용자의 회원가입 시 “데이터 정책”에 동의하도록 한 것 외에 민감정보 처리에 대한 별도의 동의를 받지 않은 것은 적법 근거가 있다고 볼 수 없으며, 이는 舊보호법 제23조제1항 위반에 해당한다.

나. 개인정보의 열람을 거절한 사실

[舊 보호법 제35조(개인정보의 열람)제3항]

신고인이 열람을 요구한 개인정보를 처리한 기간은 보호법 시행령 제41조제1항제3호의 “개인정보 보유 및 이용 기간”에 해당하고, 페이스북 로그인을 통해 개인정보가 제3자 앱에 이전된 것은 보호법 시행령 제41조제1항제4호의 “개인정보의 제3자 제공 현황”에 해당하며, 외부 활동 정보 수집 관련 동의 내역은 보호법 시행령 제41조제1항제5호의 “개인정보 처리에 동의한 사실 및 내용”에 해당한다.

따라서 피심인이 舊 보호법 제35조에 따른 열람 요구 대상에 해당하지 않는다는 등의 이유로 답변을 제공하지 않은 행위는 열람 거절의 정당한 사유로 볼 수 없으며, 舊 보호법 제35조제3항 위반에 해당한다.

다. 안전성 확보 조치를 소홀히 한 사실

[舊 보호법 제29조(안전조치의무)]

피심인은 페이스북 서비스에서 사용하지 않는 과거에 제공한 계정 복구 양식을 별다른 이유 없이 완전히 삭제하지 않았고, 이를 통한 계정 복구 요청이 정당한 이용자에 의한 요청인지 확인하지 않아 이용자 계정 정보가 해커에게 제공되었다.

이는 피심인이 개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였다고 볼 수 없어 舊 보호법 제29조 위반에 해당한다.¹⁶⁾

16) 타임라인 미리보기 사건의 경우, 개인정보 유출 경위를 검토하였을 때 피심인이 사전에 이러한 오류를 찾아내고 조치할 수 있었다고 보기 힘든 측면이 있어 명확히 보호법 위반으로 판단하기는 어려움

IV. 피심인의 주장에 대한 검토

1. 민감정보 처리의 법적 근거

피심인은 이용자 프로필의 “종교관” 및 “정치관” 필드 정보는 서비스 이용을 위해 필수적으로 요구되는 사항이 아닌 이용자가 자발적으로 기재한 것이며, 법원 판례¹⁷⁾에 따라 정보주체가 스스로 공개한 정보의 경우 舊 보호법 제23조에 따른 ‘민감정보’에 해당하지 않는다고 주장한다.

< 서울중앙지방법원 2014. 9. 11. 선고 2013고합 557, 2013고합1060(병합) 판결 >

... 검사가 빅데이터 업체로부터 제출받은 트위터 정보에는 트위터 사용자들이 트윗을 통하여 표현한 자신의 사상이나 신념, 정치적 견해 등이 포함될 수 있는 것은 사실이다. ... 이 사건 트위터 정보의 경우 정보주체가 스스로 트위터를 통하여 그 트윗의 내용을 이미 공개한 정보에 해당하는 이상 이를 위 법조항에서 정한 민감정보에 해당한다고 보기는 어렵다.

그러나, 보호법은 민감정보의 요건으로 비공개성을 요구하지 않으며, 헌법재판소는 정보주체가 공개적으로 한 행위라 하더라도 그 특성에 따라 민감정보에 해당할 수 있다고 판단하고 있다.¹⁸⁾

< 2017헌마416, 2020. 12. 23., 인용, 전원재판부 >

나. 이 사건 정보수집 등 행위의 대상인 정치적 견해에 관한 정보는 공개된 정보라 하더라도 개인의 인격주체성을 특징짓는 것으로, 개인정보자기결정권의 보호 범위 내에 속하며, 국가가 개인의 정치적 견해에 관한 정보를 수집·보유·이용하는 등의 행위는 개인정보자기결정권에 대한 중대한 제한이 되므로 이를 위해서는 법령상의 명확한 근거가 필요함에도 그러한 법령상 근거가 존재하지 않으므로 이 사건 정보수집 등 행위는 법률유보원칙을 위반하여 청구인들의 개인정보자기결정권을 침해한다.

17) 서울중앙지방법원 2014.9.11. 선고 2013고합557, 2013고합1060(병합) 판결 등

18) 헌법재판소 2020.12.23. 선고 2017헌마416 전원재판부 결정

... 이러한 야당 소속 후보자지지 혹은 정부 비판은 정치적 견해로서 개인의 인격주체성을 특징짓는 개인정보에 해당하고, 그것이 지지 선언 등의 형식으로 공개적으로 이루어진 것이라고 하더라도 여전히 개인정보자기결정권의 보호범위 내에 속한다. ... 정치적 견해가 야당 후보의 지지나 세월호 참사 관련 시국선언에 동참하면서 표현된 것으로 이미 공개된 정보이기는 하지만, 해당 정보의 민감정보로서의 성격 및 정보주체의 의도와는 무관하거나 오히려 그에 반하는 목적인 문화예술사업의 지원배제를 목적으로 피청구인들이 해당 정보를 수집·보유·이용한 점 등을 고려하면, 이 사건 정보수집 등 행위는 당초 청구인의 정보공개 목적 범위 내에서 처리된 것이라고 볼 여지도 없다.

또한, 제시된 판례는 정보의 성격과 관계없이 이용자가 자유롭게 작성할 수 있고 실시간으로 불특정 다수에게 공개되는 정보를 판단한 것으로, 해당 판례에서 피심인이 제시하지 않은 부분에는 기본적인 성격 자체가 민감정보의 성격을 갖는 것이 아니라 자유롭게 작성하는 내용에 따라 그러한 성격을 갖을 수 있는 것에 불과하므로 민감정보에 해당한다고 판단할 수 없다고 판시하고 있다.¹⁹⁾

< 서울중앙지방법원 2014. 9. 11. 선고 2013고합 557, 2013고합1060(병합) 판결 >

나아가 트위터 정보는 유전자 검사 정보, 범죄경력자료 등과 같이 해당 정보의 기본적인 성격 자체가 민감정보의 성격을 갖는 것이 아니라 해당 사용자가 자유롭게 작성하는 의 내용에 따라 그러한 성격을 갖을 수 있는 것에 불과하므로, 이러한 이유만으로 정보 전체가 민감정보에 해당한다고는 판단할 수는 없다.

이 사건 종교관·정치관의 경우 기본적인 성격 자체가 민감정보에 해당하고, 페이스북은 한정된 사람이 공유 대상이므로 공개 매체에 공개된 경우와 같다고 볼 수 없으며,²⁰⁾ 이용자 측면에서는 페이스북 프로필 작성이 통상의 서비스에 회원으로 가입·이용하면서 사업자에게 제공하는 정보로 인식할 수 있다는 점 등을 고려하였을 때, 피심인이 제시한 판례와 판단의 전제가 같다고도 할 수 없다.

19) 피심인 제시 판례는 ①현행법은 민감정보의 요건으로 비공개성을 요구하지 않는 점, ②개인정보의 요건은 비공개성을 요구하지 않는다고 판단한 것과 일관되지 못한 점, ③공개된 민감정보는 제23조 제2항 규정 적용을 못하는 점, ④트윗의 공개가 민감정보성 자체를 박탈하는 것으로 보기 어려운 점, ⑤민감정보로 보호하지 않는 것을 정보주체가 수용한 것으로 간주하기 어려운 점, ⑥폐쇄형 메신저의 경우 민감정보가 되어 동일한 정보에 대한 법적 평가가 상이하게 되는 점 등을 종합하여 현행법 해석상 타당하지 않다는 비판이 있음(송도영, “빅데이터의 개인정보 및 민감정보 여부 판단 기준”, 개인 정보 판례백선, 박영사, 2022, 제120면)

20) 서울행정법원 2023.10.26. 선고 2021구합57117 판결

< 서울행정법원 2023. 10. 26. 선고 2021구합57117 판결 >

설령 제3자 앱에 제공된 친구의 개인정보가 정보주체인 친구 스스로 페이스북 서비스를 통하여 이미 공개한 정보라고 하더라도… 원칙적으로 한정된 사람을 공유의 대상으로 하고 있다는 점에서 일반인이 일반적으로 접근할 수 있도록 외부에 공개된 매체에 공개된 경우와는 그 성질을 달리한다.

특히, 종교관·정치관 및 동성과의 결혼 정보는 舊 보호법에서 처리를 제한하는 사상·신념, 정치적 견해, 성생활 등 민감정보임이 문언상 명백하다.

피심인은 이러한 정보를 맞춤 서비스 및 광고에 이용한다고 개인정보 처리방침에만 공개하였고, 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받지 않아 이용자는 피심인의 민감정보 이용 목적 및 보유·이용 기간 등을 사전에 명확히 알 수 없었다.

따라서 이용자가 해당 정보를 자발적으로 기재하였는지 여부는 이용자에게 법정 고지사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받았는지, 법령에서 민감정보의 처리를 요구하거나 허용하는 지 등 법 위반을 판단하는데 고려 요소가 될 수 없다.

피심인은 광고 주제가 해당 주제에 대한 이용자의 잠재적 관심에 불과할 뿐 이용자의 실제 견해나 입장 등을 반드시 반영하는 것이 아니므로 ‘민감정보’에 포함되지 않으며, 이러한 정보를 법적 근거 없이 ‘민감정보’의 범위로 확장하여 인정하는 것은 법률의 엄격 해석 원칙에 반한다고 주장한다.

그러나, 이용자에 대한 ‘주관적 평가’와 부정확한 정보 또는 허위의 정보도 특정한 개인에 관한 정보이면 개인정보에 해당하고, 이에 보호법은 개인정보의 부정확 가능성을 전제로 정보주체의 정정권을 규정하고 있으며, 오히려 정보주체에 대한 ‘주관적 평가’와 부정확한 정보가 민감한 내용일 경우 상황에 따라 정보주체의 개인정보 침해 가능성이 높아질 우려도 존재한다.

또한, 위원회는 가이드라인을 통해 이용자 동의 없이 행태정보를 이용·분석하여 민감정보를 수집·생성·활용하여서는 안된다고 안내하고 있는바, 이는 피심인처럼 이용자의 행태정보를 분석하여 민감정보를 이용자 계정에 분류·관리하는 행위를 제한하는 것도 포함된다.

피심인은 광고 주제가 잠재적 관심사에 불과하다고 하나, 이용자가 “좋아요”를 누른 페이지 등 페이스북 내 활동 기록을 분석하여 도출·생성된 정보는 실제 그 이용자의 특성을 나타낼 수도 있다.²¹⁾

특히, 피심인은 이용자 행태정보 분석을 통해 이용자 계정과 민감정보에 해당하는 광고 주제를 연결하여 분류·관리하는 등 개인정보파일로 저장·관리 및 광고 타겟으로 제공한바, 이는 이용자가 열람한 콘텐츠와 유사한 콘텐츠 추천 등 통상의 맞춤형 서비스 제공을 넘어선 것으로 명백히 보호법상 민감정보 처리를 한 것으로 판단할 수 있다.

심지어 종교, 동성애, 트랜스젠더, 북한이탈주민 등 실제 도출된 주제는 이용자에 관하여 인격적·신체적·사회적 평가가 가능한 개인의 인격에 밀접히 연관된 정보이며, 이러한 민감정보가 공개되거나 광고 타겟으로 제공²²⁾되었을 경우, 이용자에 대한 부당한 차별을 유발할 수 있는 등 그 위험성²³⁾이 매우 큰바, ‘민감정보 처리’의 범위에 포함하는 것이 이용자 권리보호 및 입법 목적에 부합하므로 피심인의 주장을 수용할 수 없다.

21) 페이스북 ‘좋아요’ 분석으로 인종(95%), 성별(93%), 종교(82%), 정당(85%), 성적 지향(여성 75%, 남성 88%) 등을 거의 정확하게 분류하는바, 그 개인의 특성 반영도 가능(Private traits and attributes are predictable from digital records of human behavior, Michael Kosinski 외 2명, 2013)

22) 2012년 미국의 업체인 사가, 구매내역을 분석하여 소비자의 임신 여부를 판단하여 그에 맞는 쿠폰을 배송하였으나, 쿠폰 수신인에 10대 여고생이 포함되어있었던 사건이 있었다. 학생의 아버지는 타겟 사에 항의를 하였으나, 이후 그 학생이 실제로 임신하고 있었던 사실이 밝혀졌다.

23) 무분별하게 수집된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동이 미치는 위험성은 지대할 뿐만 아니라 개인의 인격 자체에도 치명적인 위해를 가할 수 있다(서울행정법원 2013.5.2 선고 2012구합21154 판결)

정보기술의 발달로 개인은 이제 자신이 원하지 않더라도 자신의 개별적인 생활방식이 모두 디지털화되어 흔적을 남기게 되는 것을 경험하게 된다. ... 전자적 정보처리에 의하여 개인에 관한 모든 정보가 타인에 의해 수집되어 디지털화된 데이터베이스에 저장된 만큼 개인은 자신의 모든 것이 타인에게 노출된 상태에 있게 되고, 개인이 이를 의식하는 이상 개인은 자신의 생활양식을 정하는데 크나큰 제약을 받게 된다. 이러한 상황에서 개인은 자신의 실존인격이 디지털화되어 저장된 가상인격에 의해 규정지어지게 될 우려가 크다. 이처럼 무분별하게 수집된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동이 미치는 위험성은 지대할 뿐만 아니라 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다.

2. 개인정보 열람청구 관련 대상 정보

피심인은 신고인이 열람을 요구한 사항 중 일부는 피심인이 보유하고 있지 않고 이를 보관할 의무가 없다고 주장하나, 개인정보의 제3자 제공 현황을 열람할 수 있도록 규정하고 있는 보호법 취지상 이를 합리적으로 보관할 필요성이 있다.

피심인이 제3자 앱에 대하여 페이스북 로그인을 통한 개인정보의 이전은 이용자에 의해 정보가 공유되는 것이며 개인정보 제공의 주체는 피심인이 아닌 이용자이므로 열람 요구 대상이 아니라고 주장한다.

그러나 피심인은 보유·관리하는 개인정보가 제3자 앱에 제공되는 시스템을 미리 구축해 놓는 등 정보이전 과정에서 주도적인 역할을 수행한 것으로 이용자는 정보이전 과정 전반에서 수동적이고 부차적인 역할을 하는 것에 불과하며, 소셜로그인을 통한 정보 이전에 대해 2018년 방송통신위원회는 명확히 제3자 제공임을 안내하였고, 최근 법원 또한 제3자 제공에 해당한다고 판단²⁴⁾한 바 있다.

24) 서울행정법원 2023.10.26. 선고 2021구합57117 판결

… 정보이전 과정은 메타와 제3자 앱이 메타가 보유·관리하는 개인정보가 … 제3자 앱에 제공되는 시스템을 미리 구축해놓으면, 이용자는 페이스북 로그인 방식으로 제3자 앱에 가입하는 과정에서 단순히 원고가 제공하는 화면의 ‘허가하기’를 클릭하는 것일 뿐이다. 이용자의 위와 같은 행위는 이 사건 정보이전 과정 전반에서 수동적이고 부차적인 역할을 하는 것에 불과하므로, … 메타가 정보이전 과정에서 주도적인 역할을 수행하였다는 점을 뒤집을 정도에는 이르지 않는다고 판단된다. … 원고가 친구의 개인정보를 제3자 앱에 제공한 행위는 이 사건 쟁점조항에서 말하는 ‘개인정보를 제3자에게 제공하는 행위’에 해당한다고 판단된다.

또한, 피심인은 외부활동 정보는 광고주 등이 수집하여 제공하는 정보이므로 수집 주체는 광고주 등이며 동의 및 열람 의무도 광고주 등에 있다고 주장하나, 위원회는 외부활동 정보(타사 행태정보)에 대해 피심인이 수집·이용하는 정보라고 이미 판단하였고, 제공받은 자 또한 열람 의무가 있으므로 피심인의 주장을 수용하지 아니한다.²⁵⁾

3. 개인정보 유출 관련 안전조치 의무 이행

피심인은 소스코드 배포 전 여러 테스트 과정을 거치고 있으며, 개인정보 유출을 탐지·차단하기 위한 시스템을 운영하고 있고, 정교하게 위조된 신분증이 제출되어 검토 인력이 승인한 것이며, 유출된 이용자 수가 10명에 불과하여 정보 주체의 피해가 경미한 경우로 과징금 대상이 아니라 주장한다.

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 인터넷 홈페이지를 통한 개인정보 유·노출 방지 조치의 예시로 서비스 중단 또는 관리되지 않는 홈페이지는 전체 삭제 또는 차단 조치를 명확하게 안내하고 있는바, 피심인이 사용하지 않는 비밀번호 재설정 양식을 제거하지 않고, 이를 통한 해커의 비밀번호 재설정 요구에 대해 검증 절차 없이 비밀번호를 재설정하여 알려준 것은 홈페이지를 통한 개인정보 유출 방지 조치를 소홀히 했다고 볼 수 있으나, 실제 개인정보가 유출된 이용자는 10명에 불과한 점 등을 고려하여 피심인의 과징금 미부과 의견은 수용한다.

25) 위원회는 외부활동 정보에 해당하는 타사 행태정보를 피심인이 이용자의 동의 없이 수집·이용하는 것을 이유로 舊 보호법 제39조의3제1항 위반으로 처분함(2022.9.14. 의결 제2022-014-105호)

V. 처분 및 결정

1. 시정조치 명령

개인정보 보호 및 침해 방지를 위해 피심인에 대하여 舊 보호법 제64조제1항에 따라 다음과 같이 시정조치를 명한다.

가. 이용자의 페이스북 활동 등을 통해 민감한 주제에 해당하는 광고 타겟을 생성하는 경우 이용자에게 법정 고지사항을 알린 후 별도 동의를 받는 등 보호법 제23조에 따른 적법 근거를 마련하고, 안전성 확보 조치를 취할 것

나. 이용자의 개인정보 열람 요구가 있는 경우 성실히 응할 것. 이를 위해 개인정보 제공 현황 등을 일정 기간 보관하거나, 이용자가 그 현황을 쉽게 확인·통제할 수 있도록 조치할 것

다. 처분통지를 받은 날로부터 90일 이내에 시정명령 이행 계획을 제출할 것

2. 과징금 부과

피심인의 舊 보호법 제23조(민감정보의 처리 제한)제1항 위반행위에 대해 같은 법 제39조의15제1항제3호, 시행령 제48조의11 [별표 1의5] 및 「舊 개인정보보호 법규 위반에 대한 과징금 부과기준²⁶⁾」(이하 '舊 과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 舊 보호법 제23조제1항 위반에 대한 과징금 상한액은 같은 법 제39조의15제1항제3호에 따라 위반행위와 가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 이하에 해당하는 금액으로 한다.

26) 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2020-6호, 2020. 8. 5. 제정)

나. 기준금액

1) 고의·중과실 여부

舊 과징금 부과기준 제5조제1항은 '시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리 목적의 유무, 안전성 확보조치 이행 여부 등을 고려하여 판단한다'라고 규정하고 있다.

이에 따를 때, 피심인은 영리를 목적으로 정보통신망을 통해 정보통신서비스인 페이스북 및 인스타그램 서비스를 대한민국 이용자에게 제공하고 있는 개인정보 처리자이자 정보통신서비스 제공자로서, 이용자로부터 별도 동의를 받지 않고 민감정보를 광고에 활용하는 등 이를 처리한 행위는 고의·중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있으나, 단서 조항에서 ① 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우^(제1호), ② 위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우^(제2호), ③ 이용자의 개인정보가 공중에 노출되지 않은 경우^(제3호) 중 모두에 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 규정하고 있다.

위 기준을 적용하여 피심인이 ① 광고주에게 민감정보 관련 광고 타겟 제공을 통해 직접적으로 이득을 취한 점, ② 동의 없이 민감정보를 처리한 한국 이용자의 수는 피심인이 보유한 한국 이용자 개인정보의 5%를 초과한 점, ③ 이용자의 개인정보가 공중에 노출되지 않은 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 '중대한 위반행위'로 판단하였다.

3) 관련 매출액 및 기준금액 산출

舊 과징금 부과기준 제4조제1항은 ‘관련 매출액은 위반 정보통신서비스 제공자 등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다.’라고, 같은 조 제2항은 ‘제1항에 따른 관련 매출액 산정시 서비스의 범위는 「전기통신사업법」 제5조를 기준으로 판단하되, 구체적인 판단에 있어서는 서비스 제공 방식^(제1호), 서비스 가입 방법^(제2호), 이용약관에서 규정한 서비스 범위^(제3호), 개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식^(제4호)을 고려하여야 한다.’라고, 같은 조 제3항에는 “서비스에 대한 매출액은 회계자료를 참고하여 정하되, 이를 통해 위반행위와 관련한 서비스의 매출액을 산정하기 곤란한 경우에는 해당 정보통신서비스 제공자등의 과거 실적, 동종유사 역무제공사업자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있다.”로 규정하고 있다.

피심인의 경우, 광고주가 민감정보에 해당하는 광고 타겟을 통해 페이스북 및 인스타그램 서비스에 광고를 게재할 수 있도록 하였고, 이용자의 별도 동의 없이 민감정보를 처리한 위반행위는 2022년 3월 민감정보 관련 광고 타겟을 제거함으로써 종료되었다.

따라서 관련 매출액은 피심인이 제출한 전 세계 매출액 중 기타 수입을 제외한 페이스북 및 인스타그램 서비스의 2019년, 2020년, 2021년 연평균 광고 매출액에 대한민국 이용자(월별 활성 이용자) 비율을 곱한 금액의 3개년 평균 금액을 더한 만 달러를 피심인의 관련 매출액으로 산정한다.

< 페이스북 및 인스타그램 서비스 3년간('19~'21년) 매출액 현황(단위 : 백만\$) >

구 분	2019년		2020년		2021년	
전세계 매출액						
페이스북 광고매출 비율						
인스타그램 광고매출 비율						

페이스북 광고매출액						
	한국 월간 활성 이용자 비율					
	한국 광고매출액					
인스타그램 광고매출액						
	한국 월간 활성 이용자 비율					
	한국 광고매출액					

피심인의 위반행위는 보호법 시행령 [별표 1의5] 2. 가. 1)에 따라 ‘중대한 위반 행위’에 해당하므로 부과기준율 1천분의 21을 적용, 관련 매출액에 부과기준율을 곱한 달러를 기준금액으로 산정한다.

<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

다. 필수적 가중·감경

舊 과징금 부과기준 제6조에 따라 피심인 위반행위의 기간이 2년을 초과하여 ‘장기 위반행위’에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 달러를 가중하고, 최근 3년간 舊 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 적이 있으나, 본건 위반행위는 해당 처분 이전에 종료 되었으므로 기준금액의 100분의 50에 해당하는 금액인 달러를 감경한다.

라. 추가적 가중·감경

피심인은 舊 과징금 부과기준 [별표]에 해당하는 사항이 없으므로 추가적 가중·감경을 하지 아니한다.

마. 과징금의 결정

피심인의 舊 보호법 제23조제1항 위반행위에 대한 과징금은 같은 법 제39조의 15제1항제3호, 같은 법 시행령 제48조의11 및 [별표 1의5] ‘과징금의 산정기준과 산정절차’ 2. 가. 1), ‘舊 과징금 부과기준’에 따라 위와 같이 단계별로 산출한 금액인 달러를 최종 과징금으로 결정한다.

< 과징금 산출내역 >

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
	필수적 가중 (50%,) 필수적 감경 (50%,)	추가적 가중·감경 없음 →	백만원 ²⁷⁾

3. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 및 제35조(개인정보의 열람)제3항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호 및 제10호, 舊 시행령 제63조[별표2] 및 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」²⁸⁾(이하 ‘과태료 부과기준’)에 따라 다음과 같이 부과한다.

가. 기준금액

舊 시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 舊 보호법 제29조(안전조치의무) 및 제35조(개인정보의 열람)제3항 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 적용한다.

27) 의결일(‘24.11.4.) 최초 고시 매매기준 환율(1,377.90원)을 적용하여 원화로 환산, 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

28) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2021. 1. 27. 제정)

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	舊 법 제75조 제2항제6호	600	1,200	2,400
터. 법 제35조제3항을 위반하여 열람을 제한하거나 거절한 경우	舊 법 제75조 제2항제10호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 舊 과태료 부과지침 제8조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.’라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제8조 및 [별표2] 과태료의 가중기준에 따라 舊 보호법 제29조(안전조치의무) 및 제35조(개인정보의 열람)제3항 위반행위는 ‘법 위반상태의 기간이 3개월 이상인 경우’에 해당하여 각각 기준금액의 10%를 가중한다.

2) **(과태료의 감경)** 舊 과태료 부과지침 제7조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.’라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감경기준에 따라

舊 보호법 제29조(안전조치의무) 위반행위는 ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우’, ‘보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우’에 해당하여 기준금액의 50%를 감경한다.

舊 보호법 제35조(개인정보의 열람)제3항 위반행위는 해당 사항이 없어 감경을 고려하지 아니한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 및 제35조(개인정보의 열람)제3항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,020만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반	600만 원	60만 원	300만 원	360만 원
개인정보 열람 위반	600만 원	60만 원	-	660만 원
계				1,020만 원

4. 처분 결과 공표

舊 보호법 제66조제1항 및 舊 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 ‘위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우^(제5호)’, ‘보호위원회의 처분 시점을 기준으로 최근 3년 내 시정조치 명령, 과태료, 과징금 부과처분을 2회이상 받은 경우^(제6호)’에 해당하므로 舊 보호법 제66조제1항에 따라 피심인이 과태료 부과를 받은 사실을 개인정보보호위원회 홈페이지에 공표한다.

다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.²⁹⁾

개인정보보호법 위반 행정처분 결과 공표					
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	Meta Platforms, Inc.	舊 법 제23조제1항	민감정보 처리 위반	2024.11.4.	과징금 216억13백만원 시정명령
		舊 법 제29조	안전조치의무 위반	2024.11.4.	과태료 부과 360만원
		舊 법 제35조제3항	개인정보 열람 위반	2024.11.4.	과태료 부과 660만원 시정명령
2024년 11월 4일 개 인 정 보 보 호 위 원 회					

VI. 결론

피심인의 舊 보호법 제23조(민감정보의 처리 제한)제1항, 제29조(안전조치의무) 및 제35조(개인정보의 열람)제3항 위반에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제3호, 제75조(과태료)제2항제6호 및 제10호, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 공표를 주문과 같이 의결한다.

29) 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」에 따라 공표기간 1년을 소급 적용

이의제기 방법 및 기간

피심인은 이 시정명령 및 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 11월 4일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 조 소 영 (서 명)