Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1477

안드로이드 환경에서 개인정보 처리방침의 투명성 확보방안에 관한 연구: GDPR을 기반으로*

백 인 주,† 오 준 형, 이 경 호‡
고려대학교 정보보호대학원

A Study on the Methods for Ensuring the Transparency of the Privacy Policies in Android Environment: Based on General Data Protection Regulation*

Inju Paek,† Junhyoung Oh, Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

본 연구는 EU 회원국에서 상위권을 차지하는 안드로이드 애플리케이션 50개에 대한 개인정보처리방침을 분석하여, EU 일반 개인정보 보호법(GDPR)이 규정하는 투명성 확보방안을 제시하였다. WP29 작업반에서 제시한 투명성 관련 지침을 참고하여, 개인정보처리의 투명성 확보를 위한 요소를 도출하고, 각 요소에 대한 단계별 확인 절차를 거쳤다. 그 결과, 현재 구글플레이스토어와 애플리케이션에서 각각 제공하고 있는 개인정보처리방침을 일원화하고, 개인정보처리방침을 설명하는 내용을 좀 더 이해하기 쉬운 표현으로 기술할 필요성이 제기되었다. 또한, 신속한 정보 제공 및 컨트롤러의 정보 기재 등이 개선될 필요가 있음이 제시되었다. 본 연구는 GDPR 5조 개인정보처리원칙 7가지 중 하나인 투명성의 원칙에 기반을 두어 분석하였으며, 향후 실질적인 준수를 통해 EU의 GDPR에 선제적으로 대응할 수 있는 기초 자료로 활용될 수 있을 것이다.

ABSTRACT

In this study, we analyzed the privacy policies of 50 Android applications that are on the top chart in EU members to present the methods for enhancing transparency based on GDPR (General Data Protection Regulation). Based on the guidelines in relation to transparency stipulated in WP29, this study extracted factors of transparency in order to ensure transparency of privacy data processing and carried out the verification procedures for each factor. The results revealed that the privacy policies provided in Google Play Store and applications need to be matched, the descriptions of the privacy policies need to be written in clear and plain language for readers to understand easily. and that it is necessary to provide information quickly and improve the descriptions of information which the data controller discloses. The research findings of this study could be used as a preliminary data for proactive responses to the EU's GDPR by substantially complying with the transparency of GDPR.

Keywords: privacy policy, transparency, security, GDPR, Android application

Received(10. 23. 2019), Accepted(11. 06 .2019)
* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(NO.2018-0-00261,IoT환경에서 일반개인정보보호 규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)
† 주저자, kellogg3@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

I. 서 론

2019년 초를 기준으로 안드로이드 운영체제 사용률이 전 세계 스마트폰 시장점유율의 74%를 넘어섰다[1]. 스마트폰의 편리성에 대한 사용자의 의존도가 높아지는 상황에서 개인정보보호는 더욱더 중요해지고 있다.

안드로이드 애플리케이션에 대한 개인정보 관리자는 이로써 사용자의 개인정보가 수집, 저장, 처리되는 부분에 있어 정보 주체에게 투명하고 정확하게 알릴 필요성이 있다. EU(유럽 연합회)에서도 2018년 5월 25일부터 자국민의 개인정보보호 목적으로 EU 일반 개인정보 보호법(GDPR-General Data Protection Regulation)을 시행하였다[2]. GDPR의 시행에 따라 기존 기업들의 위반 사례가 지적되면서, 각국의 개인정보처리방침에 대한 개선이 요구되고 있다.

EU 및 프랑스의 프라이버시 보호 협회인 NOYB(None of Your Business)와 LQDN(La Quadrature du Net)은 구글을 상대로 정보와 자유에 관한 국가위원회인 CNIL(Commission Nationale de l'Informatique et des libertés)에 진정서를 제출한 바가 있다[3]. 해당 이의제기서 에는 GDPR의 투명성 원칙에 대한 상세한 기술이 포함되어 있다. 접수된 불만 사항을 처리하기 위해 CNIL은 2018년 9월 안드로이드 기기를 이용하여 위반사항을 평가하였다. 평가자들은 안드로이드 상에서 구글 계정 생성할 때 사용패턴 분석하였다.

확인 결과, 구글에서 제공하는 개인정보 처리방침에 대하여 사용자가 쉽게 접근할 수 없다고 판단되었다. 데이터 처리 목적 및 저장 기간 등 필수 제공 정보를 확인하는 과정이 지나치게 복잡하며, 특히 개인 위치 정보 수집에 대한 정보는 5~6단계의 절차를 거쳐야 제공 받을 수 있는 것으로 확인되었다. 그뿐만 아니라, 제공된 항목 중 일부는 모호한 표현으로 작성되어 있으므로 투명성 원칙에 위반되었다고 판단되어 약 50만 유로의 과징금이 부과되었다[4].

안드로이드 애플리케이션 환경에서는 개인정보처리방침을 고시할 때 정확한 지침과 투명성 요소에 대한 명확한 기준이 없기에 개인정보처리방침 고시 시에 GDPR을 준수하기 위한 대응책이 부족할 수밖에 없다. 이는 애플리케이션 개발자 및 개인정보처리자

등 관계자들이 GDPR을 위반하지 않도록 대응책 마련을 요구하는 것이다.

본 연구에서는 GDPR 5조에 명시된 개인정보처리원칙 가운데 개인정보의 투명한 처리를 의미하는 '투명성'에 주목하였다. GDPR에서 투명성은 명확하게 정의되어 있지 않지만, GDPR 전문 39, WP29의 지침 내용을 통하여 그 의미를 파악할 수 있다.

해당 지침에 따르면 투명성은 애플리케이션 개발사들이 이용자에게 데이터 처리 활동을 어떻게 알리는지, 이용자 권리에 대한 커뮤니케이션은 어떻게 이루어지는지, 이용자의 권리 행사를 돕는 방법은 무엇인지 등을 다루는 요소로써, 실제 이용자의 개인 데이터에 대한 기업의 접근이 투명하게 이뤄져야 함을 의미한다[5].

이 논문[1]은 안드로이드 애플리케이션의 개인정보처리방침을 통해 GDPR의 투명성 확보방안을 도출하는 것으로, 2장은 선행연구 및 연구배경에 대하여 고찰하고. 3장은 WP29 지침을 참고하여 투명성의 요소별로 투명성 준수에 대한 기준을 세워 투명성을 확인하는 절차와 방법을 제시한다. 4장은 앞서 제시된 확인 절차와 방법을 수행한 결과를 정리한다. 마지막 5장에서는 안드로이드 환경에서 투명성 확보를 위한 방향을 제시하고 결론을 맺는다.

II. 연구배경 및 선행연구

2.1 GDPR 배경 및 투명성의 원칙

2.1.1 GDPR 배경

GDPR은 2018년 5월 25일부터 시행된 EU의 개인정보보호 법령으로, EU에 사업장을 운영하는 기업 및 EU에 거주하는 주민에게 물품 및 서비스를 제공할 경우 적용을 받는다[5]. 즉, EU 관할권 내 활동 기업뿐만 아니라 EU에 거주하는 정보 주체를 대상으로 하는 모든 기업이 GDPR의 적용을 받기 때문에, 글로벌 정보기술 기업들의 부담은 가중될 수밖에 없다.

GDPR의 개인정보처리원칙은 제2장 5조에 명시된 바와 같이 적법성·공정성·투명성의 원칙, 목적 제한의 원칙, 개인정보처리의 최소화 등 총 7개의 영역으로 구분된다[5].

이 연구에서는 GDPR의 개인정보처리원칙 가운데 투명성의 원칙에 제한하여 안드로이드 환경에서의 GDPR 개인정보보호 원칙 준수 방안을 탐색하고자

1) 백인주와 오준형은 이 연구에 동등하게 기여하였음

한다. 이는 개인정보가 처리, 저장, 수집되는 단계에서 정보 주체에게 어떠한 방식으로 이루어지고 어떻게 안전하게 처리되는지 고시해야 하는 GDPR의 의무사항을 준수하는 데 있어 투명성은 매우 중요하게 고려되는 요소이기 때문이다.

2.1.2 GDPR 투명성의 원칙

개인정보처리방침은 컨트롤러가 정보 주체에게 상호작용하는 애플리케이션에 의해 이루어지는 개인정보의 처리에 대해 고시하기 위한 수단이다. 이는 GDPR 정보 주체로부터 개인정보를 수집하는 경우 제공되는 정보인 제13조를 근거로 한다. 이때 정보 제공은 크게 의식적으로 컨트롤러에게 개인정보를 제공한 경우(온라인 서식작성 등)와 컨트롤러가 관찰을 통해 정보 주체의 개인정보를 수집하는 경우로 구분된다.

여기에서의 컨트롤러(Controller)는 개인정보의 처리 목적 및 수단을 단독 또는 공동(jointly)으로 결정하는 대상(자연인, 법인, 공공기관, 에이전시 기타 단체 등)이며, 정보 주체는 개인 데이터의 소유자, DPO(Data Protection Officer)는 데이터 보호 책임자를 의미한다[5].

GDPR의 투명성 원칙은 정보 주체에 대해 제공되는 정보가 앞에서 제시된 투명성 요소를 모두 충족할 때 준수될 수 있다.

투명성의 첫 번째 요소는 정확하고 투명하며 이해할 수 있고 쉽게 열람 가능한 방식으로 제공되어야 한다는 것으로, 선행연구에서는 이와 관련하여 정보 주체가 개인정보처리방침에 대해 피로증후군을 피할 수 있어야 한다고 주장하였다[6]. 이는 정보 주체가 컨트롤러가 제공하는 개인처리정보처리방침을 읽고 피로하거나 어렵다고 느끼지 않아야 하며, 평범한 정보 주체가 쉽게 이해할 수 있어야 하고, 정보 주체가 쉽게 정보를 찾아 열람할 수 있어야 함을 의미한다[8].

GDPR의 투명성 준수 방안을 도출하기 위해 먼저 제29조 작업반(The Article 29 Working Party, WP29)지침 내용을 참고하여 Table 1.과 같이 투명성의 요소를 정리하였다[8]. 이후 항목별로 제시된 가이드라인을 통해 준수확인 사항을 점검하였다.

2.2 선행연구

EU 관할권 내 활동 기업뿐만 아니라 EU에 거주하는 정보 주체를 대상으로 하는 모든 기업이 GDPR의 적용을 받기 때문에, 글로벌 정보기술 기업들의 부담은 가중될 수밖에 없다.

각 기업은 정보 주체들의 정보에 대하여 수집, 저장, 처리에 관한 내용을 개인정보처리방침에 담고, 투명하게 고시할 수 있도록 이바지한 이전 연구들이 존재한다.

Table 1. Factors of transparency

Factor	Description
1	Concise, transparent, intelligible, easily accessible
2	Clear and plain language
3	Providing information to children
4	In writing or by other means
5	The information may be provided orally
6	Provide free of charge

2.2.1 개인정보 처리방침의 투명성 확보방안

개인정보 처리방침이 투명하게 고시될 수 있도록 한 연구도 활발하게 진행 중이며, 기술적인 측면의 연구가 주를 이루고 있다.

Tesfay et al.(2018)은 개인정보 처리방침의 가독성 및 복잡성 문제에 주목하여, 정보 주체가 개인정보처리방침을 쉽게 읽을 수 있도록 자연어 처리 기술 및 기계학습을 사용하여 개인정보보호 정책을 단순화, 시각화한 도구인 PrivacyGuide를 개발하였다[9]. Otramari et al.(2018)은 주석이 달린 개인정보보호 정책을 나타내는 의미 체계인 PrivOnto를 개발하였다. PrivOnto는 정보 주체의 개인정보처리방침 이해를 돕기 위해 크라우드 소싱, 기계학습 및 자연어 처리의 조합을 사용하여 반자동으로 주석을 다는 정책을 기반으로 한다[10]. 개인정보처리방침의 모호성을 해결하기 위하여 심층 신경망을 사용한 Liu et al.(2016)의 연구에서는 각 방침의 내용에 포함된 조건과 조항 등에 대해 모델링과 언어 모호성을 이해할 수 있는 접근 방식이 제안되었다[11]. 이구연 외(2019)는 IoT 환경에서 GDPR의 개인정보처리원칙 준수를 위해 정보 주체의 선택적 동

의와 암호화된 개인정보수집을 통한 개인정보수집 동의 절차를 제안함으로써 투명성을 높이고자 하였다[12]. Bhatia et al.(2019)는 개인정보처리방침 내 자연어의 모호성으로 인한 개인정보 위험에 대한 정보 주체의 인식을 측정한 후, 모호성과 관련 프라이버시 위험을 식별하고 측정하는 접근법을 소개함으로써, 기업들의 개인정보처리 정책을 개선할 수 있는 메커니즘을 마련하였다[13]. Mohan et al.(2019)는 10개의 대규모 클라우드 서비스의 개인정보처리방침을 수동적으로 분석하여 잠정적으로 GDPR을 위반할 수 있는 취약점을 도출하였다. 이를 토대로 7가지 권고안을 제시하여 GDPR의 투명성 준수를 위해 개인정보처리방침의 개선이 필요함을 주장하였다[14]. 이 외에도 개인정보처리방침의 모호성을 개선하기 위한 연구, 가독성을 높이기 위한 연구가 존재한다[15], [16]. 이전 연구에서는 투명성을 확보하기 위해 크라우드 소싱, 자연어 처리 방법 등을 통해 개인정보 처리방침의 모호성을 개선하고, 가독성을 높이기 위한 연구를 수행하였다. 하지만 투명성의 요소 중 모호성이든 가독성이든, 일부분에 대해서만 해결하였기 때문에 GDPR의 전반적인 투명성이 확보되었다고 볼 수 없다. 본 연구에서는 WP29 작업반의 투명성 지침에 따른 투명성의 요소별로 절차를 세워 수동적인 분석을 진행하였다. 이에, 구체적인 지침 마련을 위한 가이드라인을 제시했다는 차별성을 갖는다.

2.2.2 안드로이드 애플리케이션의 GDPR 투명성 확보방안

안드로이드 애플리케이션에서 상에도 GDPR의 투명성 확보에 관한 연구도 활발히 진행되고 있다.

Papageorgiou et al.(2018)은 모바일 헬스(m-Health) 애플리케이션을 대상으로 과도한 권한 여부, 민감 정보가 제3국으로 이동될 때 사용하는 프로토콜, 암호화 여부 등 GDPR의 개인정보처리원칙 준수 여부에 대해 동적 및 정적 분석을 시행하였으며, 투명성에 대해 수동적으로 분석하였다. 분석 결과, 애플리케이션 중 10%는 개인정보처리방침이 없었고, 5%는 개인정보 처리방침에 대한 웹사이트는 존재하나 404 에러로 인하여, 열람할 수 없었다. 또한, 과잉 권한 부여를 하는 애플리케이션의 존재가 확인되었고, 민감 정보의 제3국 이동 시, 불안전한 프로토콜인 HTTP를 이용하는 것으로 드러났다[17]. Mangset et al.(2018)의 연구에서는 데이트 및 제약 관련 애플리케이션을 대상으로 1) 개인정보처리방침에서 데이터를 수집하는 유형에 대한 내용 도출, 2) 실제 애플리케이션 실행을 통한 데이터 수집 여부 평가, 3) 내부저장소의 암호화 여부 확인 등 개인정보처리에 있어 GDPR 준수 여부를 분석하였다. 해당 연구에서는 안전하지 않은 저장소에 민감한 정보를 저장하는 애플리케이션과 개인정보처리방침에 명시되어있지 않는 정보들을 수집하는 애플리케이션의 문제가 지적되었다[18]. 이전 연구들은 애플리케이션의 개인정보처리방침에 관한 내용이 GDPR의 투명성의 원칙에 부합하지 못함과 더불어, 수집한 개인정보를 안전하게 처리하지 못한 부분을 발견하였다. 하지만 이전 연구에서는 GDPR 제5조인 개인정보 처리원칙에 관하여 주로 연구하였으며, 개인정보처리원칙 중 하나인 투명성에 대한 평가를 한 연구는 각 연구의 전체 비중에서 일부만 차지하였다. 본 연구에서는 이전 연구와 달리 투명성을 중점적으로 분석하여, GDPR의 투명성을 확보할 방안을 마련한다는 차별성을 갖는다.

III. 안드로이드 환경에서의 GDPR 투명성 확보

3.1 데이터셋의 구성

GDPR의 투명성 원칙 준수 여부에 확인절차를 진행하기 전, 다음의 절차를 거쳐 Table 2.와 같이 GDPR에 적용되는 데이터셋을 구성하였다.

현재 앱애니(AppAnnie.com)[19]는 애플리케이션의 사용자 수를 집계해 그 순위 정보를 제공해주고 있다. 안드로이드 애플리케이션의 순위를 분석하여 정보를 제공해주는 웹사이트이며 이전 연구에서, 앱애니를 통하여 데이터셋을 구성한 이전 연구들이 존재한다[26], [27]. 본 연구에서는 앱애니의 순위 정

Table 2. Scope of dataset

Criteria	Description
1	The application should be one of the top 100 charts in EU members
2	The app must be included in the dating category of the Google Play Store.
3	Privacy policy should be written in English
4	The application must collect personal sensitive data

보를 토대로 EU 회원국 대상 애플리케이션의 개인정보처리방침을 수집하였다.

또한, GDPR의 제9조에 제시된 민감 정보를 가장 많이 포함하고 있는 애플리케이션을 조사하였다. 제9조는 민감 정보 처리원칙에 관한 조항으로 인종, 민족, 정치적 견해, 종교 및 철학적 신념, 성적 취향에 관한 정보 등 다양한 유형을 포함하고 있다.

데이트 범주는 구글플레이스토어에서 결혼, 연애, 사교 등의 목적을 가진 애플리케이션으로 분류된다. 우리는 데이트 범주 안의 애플리케이션 중 대다수가 정보 주체로부터 많은 민감 정보를 요구하는 것을 확인하였다. 반면 종교카테고리도 마찬가지로 민감 정보에 해당하였지만, 대부분은 개인정보를 수집하지 않았다. 또한, 아동을 대상으로 개발된 교육카테고리의 애플리케이션의 경우는 아동의 개인정보를 수집하지 않으며 대상자의 부모를 위한 개인정보처리방침이 전반적으로 존재하였다.

이에, 상위 순위에 포함된 데이트 관련 애플리케이션에 한정하여 연구를 진행하였다. 개인정보처리방침의 원활한 분석 및 가독성 실험을 진행하기 위해 개인정보처리방침의 영문으로 작성된 범주로 한정하였다. 마지막으로는 개인정보를 처리하고 있는 애플리케이션을 대상으로 하였다.

위 절차에 따라 최종적으로 50개의 애플리케이션이 연구대상으로 선정되었고, 각 애플리케이션의 개인정보처리방침을 수집하였다. 각 애플리케이션을 조사하기 위한 환경으로는 IP주소를 우회하여 법 관할 지역인 프랑스 지역으로 설정한 상태에서 분석을 진행하였다. 구글플레이스토어를 통해 습득한 개인정보처리방침이 실제 애플리케이션 상에서 보이는 개인정보처리방침과 다를 수 있으므로, 두 가지의 방식으로 이를 확인하였다.

먼저 구글플레이스토어에 고시된 애플리케이션의 개인정보처리방침이 있는 웹사이트의 이동하여 개인정보 처리방침을 확인하였다. 그리고 애플리케이션을 직접 설치하여 회원가입 전후에 나오는 개인정보 처리방침을 분석하였다. 자료 수집에 사용된 기기는 갤럭시 S8((SM-G950)이었으며, GDPR 시행 이후인, 2019년 6월 13일에 데이터를 수집하였다.

3.2 투명성의 원칙 준수확인 방법

투명성의 원칙 준수 여부를 확인하기 위하여 제29조 작업반이 제시한 투명성 의무에 대한 지침을 참고하여 절차대로 방법을 제시하였고, 단계별로 확인작업을 진행하였다.

Table 3. Information which must be provided to a data subject

Category	Required information Type
1	The identity and contact details of controller
2	Contact details of the DPO(data protection officer)
3	Legal basis and purposes for the data processing
4	Where legitimate interests is the legal basis for the processing, the legitimate interest pursued by the data controller or a third party
5	Recipients of the personal data
6	Details of transfers to third countries, and safeguards
7	The storage period
8	The rights of the data subject to access, rectification, erasure, restriction and objection on processing, portability
9	The right to withdraw consent at anytime
10	The right to lodge a complaint with a supervisory authority
11	The existence of automated decision-making and, if applicable, meaningful information about the logic used

본 연구는 컨트롤러가 정보 주체로부터 개인정보를 직접 수집해야 하는 경우, 정보 주체에게 제공해야 하는 정보를 제13조를 참고하여, Table 3.과 같이 11가지의 기준점을 정리하였다[20].

개인정보처리방침의 존재 여부, 구글플레이스토어 상에서 이동되는 개인정보처리방침 관련 웹사이트의 상태 확인 결과를 통해 접근에 대한 용이성을 증명하였다. 이후 개인정보처리방침에 대해 컨트롤러가 데이터 주체에게 고시해야 하는 정보가 있는지 확인하였다. 이때 개인정보처리방침에 관한 내용이 부재 시, 이용약관 및 해당 홈페이지를 통해 확인하였다.

다만, 본 연구에서는 11번의 프로파일링에 관한 내용은 연구자가 실제 프로파일링을 하는지에 대하여 육안상 확인하는데 한계점이 존재하였다. 11번에 대한 고시가 되어있지 않을 경우, 원인 파악이 불가하였다. 따라서 이 항목은 연구대상에서 제외하였다.

3.2.1 간결하고 투명하며, 이해할 수 있고 쉽게 접근 가능하며, 열람 가능한 방식

본 연구에서는 첫 번째 요소인 간결하고 투명하며, 이해할 수 있고 쉽게 접근 가능하며, 열람 가능한 방식의 준수 여부를 확인하기 위하여 개인정보처리방침의 목차가 있는지 확인하였다. 개인정보처리방침은 주로 특정 형식만 먼저 보여주고, 정보 주체가 필요한 항목을 선택할 경우, 해당 조항이 존재하는 쪽으로 이동이 되거나 숨겨있던 내용이 펼쳐지는 경우로 나뉜다.

더불어 접근에 대한 용이성 확인을 위해 애플리케이션에 개인정보 처리방침이 알림창에 뜨는지, 챗봇을 통하여 정보를 얻을 수 있어 즉각적이고 명확한 열람이 가능한지 확인하였다.

3.2.2 분명하고 쉬운 언어 사용

개인정보처리방침이 분명하고 쉬운 용어를 사용하고 있는지 확인하기 위해 WP29의 기준을 참고하여, 모호성 실험과 가독성 실험을 진행하였다.

3.2.2.1 모호성 실험

WP29 작업반에서는 개인정보처리방침의 모호성에 대하여 구체적이고, 명확하지 않은 용어로 작성되어 있거나, 정보 주체로부터 다른 해석의 여지를 주어 혼동할 가능성이 있는 의미로 해석하였다[8].

따라서 우리는 개인정보 처리방침에서 모호한 표현이 얼마큼 존재하며, 어떤 부분이 모호한지 파악하기 위해 WP29가 제시한 사례 및 개인정보처리방침 내용에 대한 모호성 실험을 한 선행연구를 참고하여 확인하였다[13], [21], [22]. WP29 지침 내에 모호한 표현 예시로는 *"새로운 서비스를 개발하기 위해 귀하의 개인정보를 사용할 수 있습니다", "맞춤형 서비스를 제공해주기 위해 귀하의 개인정보를 사용할 수 있습니다"*라는 표현을 모호하다고 제시하였다. 이 문장의 경우는, 새로운 서비스 및 맞춤형 서비스가 어떤 내용임을 지칭하는지 불명확하므로 투명성의 두 번째 요소에 부합하지 않는 것으로 간주하였다.

또한, 개인정보처리방침을 분석하여 모호한 용어를 추출한 후, 각 모호한 단어와의 상관관계를 분석한 Reidenberg et al.(2016)의 논의를 참조하였다[21]. 이 연구에서 제시한 모호한 용어의 범주는 총 4가지로 구분되며, Table 4.와 같다.

Table 4. Table of Vague terms adopted from (Reidenberg et al. 2016)

Category	Vague term
Modality	may, can, would, might, could, possibly
Quantifier	certain, most, some
Generality	typically, normally, often, general, usually, generally, commonly, among other things, widely, primarily, largely, mostly
Conditionality	as needed, as necessary, as appropriate, depending, sometimes, as applicable, otherwise reasonably determined, from time to time

양태(Modality) 범주 안의 단어가 포함된 문장의 예시를 살펴보면, *"다른 마케팅 목적으로 미래에 정보를 공개할 수도 있다"*를 들 수 있다.

예시 문장의 경우 목적이 명확하지 않고, 쓸 수 있을지도 확실하지 않기 때문에 모호한 용어로 간주하였다. 정량자(Quantifier) 범주 내 용어인 some, most는 어떠한 대상의 일부를 나타내며 명확한 대상이 아닌 대략적인 부분을 표현할 때 쓰는 단어이다. 또한, 일반화(Generality) 범주 내에는 보통이란 뜻의 usually, 일반적이란 뜻의 generally 등의 단어가 있다. 개인정보처리방침 내 예문으로는 *"개인정보는 보통 6년에서 삭제된다"*가 있다. 이 부분에서 '보통'은 정보 주체자가 정확히 본인의 정보가 삭제되는 시기를 대략적으로밖에 알 수가 없으므로 모호하다는 기준이 되었다. 마지막으로 조건문(Conditionality)인 as needed, as necessary도 미래에 대한 가정이며, ~일수도 아닐 수도 있다는 추상적인 단어에 해당하므로 모호한 단어에 기준이 되었다.

우리는 개인정보처리방침의 내용 중, 데이터수집, 저장, 공유에 관한 내용을 추출하였다. 그 이후, 위 선행연구에서 말한 모호한 용어가 쓰여, 모호하게 해석되는 문장의 비중을 확인하였다.

우리는 모호한 용어가 사용된 문장 모두를 모호한 표현이라고 간주하지 않았다. 해당 문장이 추상적인 표현인지를 가려내기 위하여, 용어가 문장상에서 어떻게 해석되는지 확인하였다. 또한, 모호한 표현이

사용된 문장의 다음 문장까지 분석하였다.

예를 들어 may는 다중적인 의미가 있다. 가능성을 나타낸 '~일지도 모른다'로 해석될 경우 모호하다고 간주하였지만 '~해도 된다', '5월' 등의 표현으로 해석되면 제외하였다. 또한, 조건문 용어인 'as needed'의 경우 모호한 단어이지만, 그다음 문장에 앞의 내용에 대한 구체적 예시가 주어진 경우는 제외하였다.

3.2.2.2 가독성 실험

우리는 개인정보처리방침이 얼마나 읽기 쉽게 되어있는지를 정량적인 지표를 평가하기 위하여 가독성 실험을 진행하였다. 이전 연구에서는 영어 단어 기준으로 음절의 수, 문장 내의 단어 개수 등을 측정하여, 문장의 복잡한 정도를 수치화시킨 특정 기법들이 존재한다[23], [24].

우리는 가독성 난이도를 측정하기 위하여 플레시 가독성 점수(Flesch Reading Ease score)실험과 플레시-킨케이드 학년 수준(Flesch-Kincaid Grade Level)실험을 통해 각 개인정보처리방침 내용에 대하여 가독성 평가 결과를 도출하였다.

플레시 가독성 점수(Flesch Reading Ease score)는 단어 길이 및 문장 길이에 의해 독해 난이도를 계산하는 공식을 이용하며, 수치가 0부터 100까지 산출된다. 점수가 높을수록 문장의 이해가 쉬우며, 미국을 기준으로 90~100점이면 11살이 쉽게 이해할 수 있다. 60~70점은 보통 13세~15세 학생이 이해할 수 있는 정도를 뜻하며 0~30점은 대학교 학위 취득자들 이상의 사람이 대게 이해할 수 있다는 지표로 활용된다.

플레시-킨케이드 학년 수준(Flesch-Kincaid Grade Level)은 미국 학생 학년을 지표로 하며, 단어당 음절 수 및 문장 당 단어 수를 이용하여 읽기 수준을 계산한 방법이다. 등급은 0~18까지 있으며 등급이 높을수록 읽기가 어려움을 의미한다[25].

우리는 각 개인정보처리방침을 평가하여, 평균값, 최댓값, 최솟값으로 데이터셋의 전반적인 가독성 결과를 파악하였다.

3.2.3 서면 제공 또는 그 밖의 수단으로 제공

서면 제공 또는 그 밖의 수단으로 제공되는지를 확인하기 위하여 분석대상 애플리케이션들에 대해 현재 개인정보 처리방침 구조가 서면으로 되어있는지 일차적인 확인을 거친 후, 다른 방법의 고지가 이루어지고 있는지를 확인하였다.

GDPR은 전자적 수단 등 기타 특정되지 않은 수단을 통한 고지를 권고 사항에서 구체적으로 허용하고 있다. 정보 주체들이 관심 있게 볼 방법을 시간에 맞춘(just-in-time) 방법, 팝업 고지, 마우스 커서를 이동해서 보는 호버오버(hover-over) 고지 등의 전자적 수단이 해당한다.

다만 본 연구에서 투명성의 원칙과 관련하여 다음의 요소들에 대한 분석은 시행하지 않았다.

먼저 아동 및 취약 계층에 정보 제공 시, 대상에 적합한 적절하고 공감되는 어휘, 어조, 언어 스타일을 사용하는지는 분석하지 않았다. 구글플레이스토어에서 분류한 교육 범주의 애플리케이션들의 주요 이용 고객은 13세 미만의 아동들로, 본 연구의 분석대상인 18세 이상 성인이 이용 가능한 데이트 관련 애플리케이션에 해당하지 않기 때문이다.

더불어 정보의 구두 제공 여부와 무상 제공 여부 역시 별도로 분석하지 않았다. 구두 제공 여부의 경우, 전화번호가 아니더라도 우편, 전자우편 등을 통해 음성 전달이 가능하므로 분석 결과의 객관성을 담보하기 어렵기 때문이다. 또한, 무상 제공 여부에 대해서도 분석 대상인 데이트 관련 애플리케이션뿐만 아니라 전수조사를 통해 확인된 다른 범주의 애플리케이션 역시 현재까지 정보 확인에 따른 발생 비용이 없는 것으로 확인되었기 때문에 분석에는 포함하지 않았다.

이상의 논의를 토대로 본 연구에서는 투명성의 6가지 요소 가운데 3가지 요소(간결하고 투명하며, 이해할 수 있고 쉽게 접근 가능하며, 열람 가능한 방식, 분명하고 쉬운 언어 사용, 서면 제공 또는 그 밖의 수단으로 제공)에 한정하여 투명성 준수 여부를 확인하였다.

IV. 실험결과

우리는 개인정보처리방침, 이용약관, 애플리케이션의 홈페이지 확인을 통해 안드로이드 애플리케이션의 개인정보처리방침이 GDPR에서 제시하는 제공 정보를 포함하고 있는지를 확인하였다.

먼저 정보 주체에게 개인정보를 직접 수집하는 경우 13조에 명시된 컨트롤러가 정보 주체들에게 제공해야 할 10가지 기준에 대한 정보가 충분히 고지되

Table 5. The number of applications provided to the data subject

Category	1	2	3	4	5	6	7	8	9	10
Number	44	21	45	28	30	30	40	28	33	26

고 있는지를 확인한 결과는 Table 5.에서 설명한다.

각 애플리케이션에서 정보 주체에게 제공되는 정보는 총 10개의 항목 중 평균 6.2개가 제공되고 있었다. GDPR은 DPO를 지정하여, 신원 및 연락처를 제공할 것을 명시하고 있는데, 분석대상 50개 애플리케이션 가운데 21개의 애플리케이션만이 DPO의 신원 및 연락처를 제공하고 있음이 확인되었다.

반면, 해당 개인정보의 처리 목적 및 처리의 법적 근거, 컨트롤러의 신원 정보 등은 분석대상 애플리케이션 중 45개(약 90%)에서 제공되고 있는 것으로 파악되었다. 또한, 10개의 항목모두 존재하는 경우는 총 14개이며 28%를 차지한다. 반면에 모든 정보가 존재하지 않는 경우는 한 개의 애플리케이션이 존재하였다.

다음으로 애플리케이션 상에서 회원가입을 기준으로 정보 주체가 개인정보처리방침을 확인할 수 있는 시점을 분석한 결과는 Table 6.과 같다.

애플리케이션 상에서 개인정보 처리방침이 부재한 경우가 1건이었으며, 이용약관만 있거나 개인정보만 있는 경우가 3건이 있었다. 이 경우를 제외하였으며, 회원가입 이후에 확인 가능한 경우가 8건이었다. 이는 데이터 주체가 개인정보를 제공한 이후, 방침을 확인할 수 있는 상황에 해당한다.

Table 6. Available time to check privacy policy

Before sign up	After sign up	Absence of privacy policy
38	8	4

4.1 간결하고 투명하며, 이해할 수 있고 쉽게 접근 가능하며, 열람 가능한 방식

WP29 작업반에서는 개인정보처리방침 중 특정 부분에 대한 즉각적인 열람을 권고하고 있다. 본 연구에서는 개인정보처리방침에 게시된 글의 전체적인 구조를 살펴보고, 특정 부분의 열람 가능 여부, 목차의 유무를 파악하였다.

4.1.1 접근 및 이동 용이성

한편, WP29에서는 이러한 개인정보들이 일반 사용조건 등 관련 정보와 차별화되어야 한다고 명시하고 있다. 이와 관련하여 개인정보처리방침이 이용약관과 별개로 작성되어 있는지를 살펴보았다, 그 결과, 이용약관만 있고 개인정보처리방침이 없으며, 개인정보보호 관련 내용의 일부만이 존재하고 있는 애플리케이션은 3건, 이용약관 안에 개인정보처리방침이 함께 존재하는 경우는 2건으로 일반 이용약관 사항과 차별화되지 않은 부분들이 확인되었다.

더불어, 쉽게 접근할 수 있는지 알기 위해 적절한 개인정보처리방침의 내용 제공 여부와 접근성 여부를 확인하였다. 그 결과 모든 애플리케이션이 개인정보처리방침을 고시하고 있으나, 구글플레이스토어에서 내려받은 개인정보처리방침과 실제 애플리케이션의 회원가입 전후로 보이는 개인정보처리방침의 내용이 다른 경우가 7건이었다.

구체적으로 애플리케이션 상과 구글플레이스토어의 링크를 통해 연결되는 웹사이트가 다른 경우가 확인되었다. 데이터셋 중 eharmony애플리케이션이 이러한 결과의 예시이다. Fig.1.은 eharmony의 개인정보처리방침에 대한 내용이다. 왼쪽은 구글플레이스토어 상의 링크(*https://www.eharmony.com/privacy/policy*)로 연결된 화면을 보여주고, 오른쪽은 애플리케이션 설치 후 이동되는 링크(*https://www.eharmony.co.uk*)로 연결된 화면을 보여준다. 이동되어지는 웹사이트가 다를 뿐만 아니라, 개인정보처리방침에 대한 구성 목차도 다른 것이과 같이 확인되었다.

애플리케이션 상에는 총 16개의 목차로, 적용 범

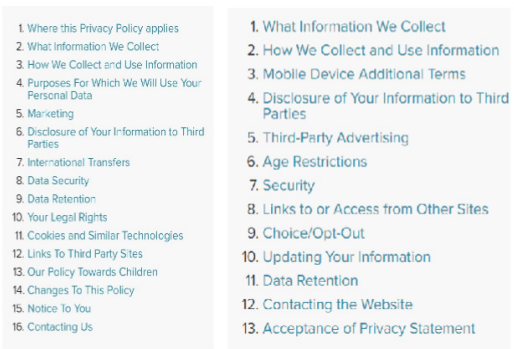

Fig. 1. Privacy policy of eharmony application

위, 마케팅, 고지사항 등 비교적 상세한 내용이 포함되어 있으며, 이는 구글플레이스토어에서 이동되는 목차보다 3개 더 많았다. 구글플레이스토어의 개인정보처리방침은 정보 주체에게 제공해야 할 정보 10개 중 4개의 내용만 존재하는 반면, 애플리케이션 상에서는 모든 내용이 존재하고 있었다.

이처럼 구성 및 내용이 다른 경우는 3건이었으며, 애플리케이션 상에는 개인정보처리방침이 존재하나 404 에러로 구글플레이스토어를 통해 개인정보처리방침 관련 사이트로의 이동할 수 없는 경우 2건, 구글플레이스토어에서는 개인정보처리방침의 내려받을 수 있었지만, 애플리케이션 상에서는 개인정보처리방침이 존재하지 않는 경우 2건이 있었다. 대표적인 예로는 데이터셋 중 Inshallah 애플리케이션이 존재하였다. Fig.2.는 Inshallah 애플리케이션의 개인정보처리방침예시이다. 왼쪽은 애플리케이션 설치 전의 구글플레이스토어 화면이며, 오른쪽은 구글플레이스토어를 통해 개인정보처리방침을 선택하여 연결된 웹사이트 창이다. 좌측 하단 부분에는 이동된 구글플레이스토어에서 개인정보 처리방침 관련 웹페이지로 이동 시, 개인정보처리방침과 무관한 내용이 기술된 경우이다.

또한, 이동된 웹페이지 내에 개인정보처리방침의 존재가 확인되었으나, 이는 이용약관에 관한 내용이며, 모바일 애플리케이션에 보안지침이 일부만 존재하였다.

따라서 컨트롤러와 DPO에 의해 정보 주체가 개인정보처리방침에 접근할 수 있는 방식의 일원화가 필요할 것으로 판단된다.

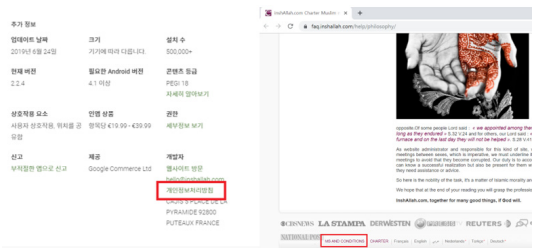

Fig. 2. Inshallah privacy policy by reaching Google Play Store

4.1.2 즉각 열람 방식

즉각적으로 열람할 수 있도록 목차를 처음에 제시하는 방법은 세 가지로 구분할 수 있다. Fig.3.은

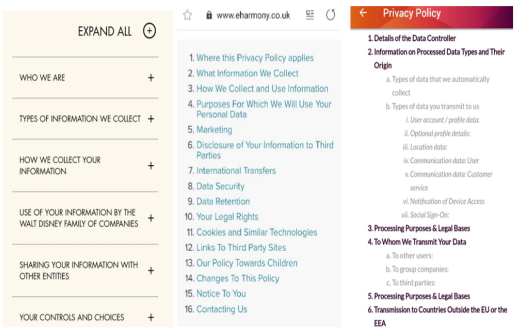

Fig. 3. Privacy policy of Disney junior play, Okcupid, Koko application

왼쪽부터 Disney Junior Play, Okcupid, Koko의 개인정보 처리방침의 예시이다. 목차 선택 시 숨겨져 있던 밑의 내용이 드러나는 경우((Disney Junior Play 등), 목차 선택 시 해당 정보가 있는 내용으로 이동되는 경우(Okcupid 등), 목차 선택 시 별도의 클릭을 통해 원하는 내용으로 이동이 가능한 경우(koko 등)이다.

열람 방식의 투명성을 확인하기 위하여 애플리케이션 상에서 회원가입 전에 제공되는 개인정보처리방침에 관한 내용을 분석하였다. 확장하기 버튼 선택 시 숨어져 있던 내용이 펼쳐지는 방식의 개인정보처리방침은 0건, 즉각 열람할 수 있도록 목차를 처음에 제시하고 원하는 정보 선택 시 해당 정보로 이동 가능한 개인정보처리방침은 3건이었고, 목차를 보여주지만, 해당 정보로의 이동할 수 없는 개인정보처리방침은 1건이 있었다.

4.2 분명하고 쉬운 언어 사용

4.2.1 모호성 실험

각 애플리케이션의 개인정보처리방침에 대해 개별적으로 내용상 자료 수집, 저장, 공유, 보유 기간에 관한 내용만 도출하여 모호한 용어 및 모호한 용어가 포함된 문장을 추출하였다. 해당 내용을 포함하고 있지 않은 8개 애플리케이션을 제외한 42개 애플리케이션을 대상으로 살펴본 결과는 다음의 Table 7.과 같다. 8개의 개인정보처리방침에는 양태범주 안에 있는 용어가 포함되었다. 4개의 방침에서는 조건문 안에 용어가 포함되고 있었으며, 2개의 방침에는 일반성에 포함된 용어가 존재하였다.

Table 7. Results of ambiguity Test

Category	Frequency
Modality	8
Conditionality	4
Generality	2

4.2.2 가독성 실험

분명하고 쉬운 언어 사용이 이루어지고 있는가에 대해서는 플레시 가독성 점수 및 플레시-킨케이드 학년 수준를 통한 가독성 실험을 진행하였다[15].

먼저 Flesch-Kincaid Grade Level을 분석한 결과, 연구대상 50개 애플리케이션의 가독성 평균은 12.6이었고, 3개의 애플리케이션이 가장 높은 레벨인 15로 나타났으며 총 3개의 애플리케이션이 있었으며, 가장 낮은 레벨은 8.9로 1개의 애플리케이션이 해당하였다. 이는 분석대상 50개 애플리케이션이 평균적으로 어린아이도 쉽게 읽을 수 있을 정도의 가독성이 있음을 의미한다. 가독성을 실험한 결과는 다음의 Table 8.과 같다.

Flesch Readable Score는 수치가 높을수록 쉽게 읽을 수 있음을 의미하는데, 분석대상 애플리케이션 가운데 16개의 개인정보처리방침이 30점대로 나타났다. 이러한 결과는, 연구대상인 데이트 관련 애플리케이션 개인정보처리방침의 내용이 가독성은 높은 편이나, 누구나 이해하기는 어려운 성격, 즉, 평이성을 충족하지 못하고 있음을 보여준다.

Table 8. Result of readability test

Category	Flesch-Kincaid Grade Level	Flesch Reading Ease
Average	12.6	40.3
Minimum	8.9	49.8
Maximum	15	31.5

4.3 서면 또는 그 밖의 수단으로 제공

개인정보처리방침이 서면 또는 이외의 수단으로 제공되고 있는지를 확인한 결과는 4.1과 겹치는 부분이 있는 것으로 나타났다.

현재 개인정보 처리방침 구조가 서면으로 되어있는지 일차적인 확인을 거친 후, 다른 방법의 존재 여부를 확인하였다. 푸시(Push) 및 풀(Pull) 고지 가이드라인, 시각화 도구인 아이콘 등을 활용하여 애플리케이션별 제공 수단의 유형을 확인하였다. 이용약관과 같이 있는 내용은 제외하였다. 애플리케이션을 설치하면 나오는 개인정보처리방침과 설치 전, 구글 플레이스토어에서 연결되는 링크와 다를 경우는 애플리케이션을 기준으로 확인하였다.

확인 결과는 Table 9.과 같다. 모든 개인정보처리방침은 서면으로 제공되고 있었으며, 푸시 및 풀 고지 등 정보 주체의 관심을 유도하는 별도의 방침은 존재하지 않았다. 하지만 구조 내부에 일부 아이콘을 사용하여 시각화를 돕는 애플리케이션은 총 2개가 존재하였으며, 아이콘이 아니더라도 수집방법에 대하여 표로 명확하게 게시한 방침도 2개가 존재하였다.

Table 9. The results of provision method of privacy policy

Provision method	Digital context	Layered	Icon	Hover and over
Number	50	49	2	0

V. 결 론

이 논문에서는 GDPR이 명시한 개인정보처리원칙 가운데 투명성의 원칙이 안드로이드 환경에서 실제 준수되고 있는지를 확인하기 위해 투명성 요소를 구분하고, 각 요소에 대한 투명성 준수 확인절차 및 방법을 제시하였다.

분석 결과, 투명성을 위반할 수도 있는 많은 요인이 존재하였다. 개인정보처리방침이 이용약관과 차별화되어, 별개로 존재해야 한다는 GDPR의 권고가 제대로 수용되지 않고 있는 애플리케이션이 확인되었다. 또한, 대다수 애플리케이션이 투명성의 두 번째 요소인 분명한 표현과 평이성을 충족시키지 못하고 있는 것으로 나타났다.

본 연구의 논의는 다음과 같다.

첫째, 정보 주체에게 정보 공개를 많이 하지 않는 애플리케이션들의 최신 버전 개인정보처리방침은 GDPR 관할 이전에 수립된 경우가 많았다. 이는 GDPR의 규정에 따라 개인정보처리방침의 내용을 변경, 알릴 필요성을 보여준다.

둘째, 개인정보 처리방침의 모호한 표현으로 인해 정보 주체의 혼동을 예방하기 위해서는 구글플레이스

토어 상의 개인정보처리방침과 애플리케이션 상의 개인정보처리방침의 내용을 일원화할 필요가 있다.

셋째, 개인정보를 수집할 경우 컨트롤러가 데이터 주체에게 제공해야 할 정보를 개인정보처리방침의 내용에 포함하여 고지할 경우, 투명성 수준을 높일 수 있을 것으로 판단된다.

다만 본 연구는 투명성에 제한하여 살펴본 것이기 때문에 7개의 원칙 전부에 대해 다루지 않았으며, 데이트 범주에 속한 50개 애플리케이션만을 분석하였다. 따라서 본 연구에서 제시된 확인 절차를 모든 원칙에 확대 적용하기가 어렵다는 한계를 갖는다. 안드로이드 애플리케이션의 정보 주체는 개인정보에 있어 마땅히 보호받을 권리가 있으며 컨트롤러와 DPO는 이를 보장하기 위해 노력할 의무를 갖는다. EU의 GDPR은 이러한 권리와 의무를 명시한 것이지만, 현재까지 법적 위반에 대한 명확한 기준이 부재하다. 따라서 투명성의 원칙을 준수할 수 있는 기준과 준수를 위한 절차 마련이 필요한 실정이다.

이에 절차별로 준수 여부를 확인한 본 연구의 결과를 바탕으로 후속 연구가 진행된다면, 투명성 원칙 준수 강화 방안이 마련되어 애플리케이션 개발 및 제공자가 GDPR을 준수하는 토대가 마련될 것으로 기대한다.

References

[1] statcounter, https://gs.statcounter.com/os-market-share/mobile/worldwide, 2019

[2] Son, Young Hoa and SooJin Son, "Korean Companies' Response to the EU General Data Protection Regulations (GDPR)," *The Journal of Comparative Private Law*, 26(1), pp. 413-452, 2019.

[3] Noyb, Plainte au titre de l'article 77 (1) du RGPD, https://noyb.eu/4complaints, 2019

[4] CNIL, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", 2019.

[5] General Data Protection Regulation, Regulation (2016) 2016/679 of the European Parliament and of the Council, Regulation (EU) (2016, 679)

[6] Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung. "The role of privacy fatigue in online privacy behavior," Computers in Human Behavior, vol.81, pp. 42-51, 2018.

[7] Tesfay, Welderufael B., et al. "Privacy Guide: towards an implementation of the EU GDPR on internet privacy policy evaluation," Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics. ACM, 2018.

[8] WP29. Guidelines on transparency under Regulation 2016/679, December 2017.

[9] Tesfay, Welderufael B., et al. "Privacy Guide: towards an implementation of the EU GDPR on internet privacy policy evaluation," Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics. ACM, 2018.

[10] Oltramari, Alessandro, et al. "PrivOnto: A semantic framework for the analysis of privacy policies," Semantic Web, vol.9, no.2, pp. 185-203, 2018.

[11] Liu, Fei, Nicole Lee Fella, and Kexin Liao. "Modeling language vagueness in privacy policies using deep neural networks," 2016 AAAI Fall Symposium Series, 2016.

[12] Lee, Goo Yeon, Bang, Jun Il, Cha, Kyung Jin and Kim Hwa Jong, "GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment," *Journal of Korean Institute Of Information Technology*, 17(5), pp. 129-136, 2019.

[13] Bhatia and Jaspreet, "Ambiguity in Privacy Policies and Perceived Privacy Risk," Diss. figshare, 2019.

[14] Mohan, Jayashree, Melissa Wasserman, and Vijay Chidambaram. "Analyz

ing gdpr compliance through the lens of privacy policy," arXiv preprint arXiv, 2019.

〔15〕 Singh, Ravi Inder, Manasa Sumeeth, and James Miller. "Evaluating the readability of privacy policies in mobile environments," *International Journal of Mobile Human Computer Interaction (IJMHCI,* vol.3, no.1, pp. 55-78, 2011.

〔16〕 Yu, Le, et al. "Autoppg: Towards automatic generation of privacy policy for android applications," Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, 2015.

〔17〕 Papageorgiou, Achilleas, et al. "Security and privacy analysis of mobile health applications: the alarming state of practice," IEEE Access, vol.6, pp. 9390-9403, 2018.

〔18〕 Mangset and Peder Lind, "Analysis of Mobile Application's Compliance with the General Data Protection Regulation (GDPR)," MS thesis. NTNU, 2018.

〔19〕 appannie.com, https://www.appannie.com/kr/, 2019

〔20〕 KISA, https://www.kisa.or.kr/business/gdpr/gdpr_tab1.jsp

〔21〕 Reidenberg, Joel R., et al. "Ambiguity in Privacy Policies and the Impact of Regulation," *The Journal of Legal Studies, vol.45*, no.S2, 2016.

〔22〕 Schaub, Florian, Rebecca Balebako, and Lorrie Faith Cranor. "Designing effective privacy notices and controls," IEEE Internet Computing, 2017.

〔23〕 Spache and George, "A new readability formula for primary-grade reading materials," *The Elementary School Journal,* 53.7, pp. 410-413, 1953.

〔24〕 Kincaid, J. Peter, et al. "Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel," 1975.

〔25〕 Milne, George R, Mary J. Culnan, and Henry Greene. "A longitudinal assessment of online privacy notice readability," *Journal of Public Policy & Marketing,* vol.25, no.2, pp. 238-249, 2006.

〔26〕 Kummer, Michael, and Patrick Schulte, "When private information settles the bill: Money and privacy in Google's market for smartphone applications." Management Science, 2019.

〔27〕 Simon and Jean Paul, "How Europe missed the mobile wave." vol.18, no. 4, pp. 12-32, 2016

〈저자소개〉

백 인 주 (Inju Paek) 학생회원
2015년 2월: 서울여자대학교 정보보호학과 졸업
2018년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 프라이버시, IoT보안, 블록체인

오 준 형(Junhyoung Oh) 학생회원
2017년 2월: 고려대학교 전기전자전파공학부 졸업
2017년 3월~현재: 고려대학교 정보보호대학원 석·박사 통합과정
〈관심분야〉 정보보호, 위험관리, 프라이버시

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보보호대학원 박사 졸업
2017년 2월~2019년 2월: 고려대학교 정보전산처장
2011년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 정보보호 정책, 개인정보보호 정책, 위험관리, 머신러닝, 블록체인