# 사용자 친화형 모바일/웨어러블 센서 데이터 수집 시스템 파일럿 디자인 연구

장진혁[1], 이현수[2], 이의진[3]

한국과학기술원 전산학부[1], 한국과학기술원 지식서비스공학대학원[2],

한국과학기술원 산업 및 시스템 공학과[3]

jhjangbot@kaist.ac.kr, hslee90@kaist.ac.kr, uclee@kaist.ac.kr

# Pilot System Design Study for User-Friendly Mobile/Wearable Sensor Data Collection

*Jinhyuk Jang*[1], *Hyunsoo Lee*[2], *Uichin Lee*[3]

*School of Computing, KAIST*[1],

*Graduate School of Knowledge Serving Engineering, KAIST*[2],

*Industrial & Systems Engineering, KAIST*[3]

**요 약**

모바일 및 웨어러블 기기의 사용이 늘어나면서 사용자의 "라이프로그 데이터" 수집이 늘어났다. 데이터의 수집으로 인해 사용자들은 보다 편한 서비스를 이용할 수 있는 대신, 24시간 센싱을 통해 지속적으로 수집되는 데이터의 방대한 양 및 다양한 데이터 종류로 인해 개인정보 유출 및 사생활 침해의 위험에 노출되었다. 이러한 개인 프라이버시 위협에도 불구하고 현재 개인정보 보호방침은 사용자가 이해하기 어렵게 작성되어 있으며 사용자가 주도적으로 데이터 수집에 동의하고 데이터를 관리하기 어렵게 설정이 되어 있다. 본 연구는 현재 센서 기반 어플리케이션의 개인정보 보호방침 제공 방식 및 사용자 친화적 데이터 수집을 위한 시스템 디자인 파일럿 스터디를 수행하였다.

## 1. 서 론

최근 일상생활 속 개인과 모바일 및 웨어러블 기기 간 상호작용을 통하여 수집되는 "라이프로그 데이터"의 활용에 대한 관심이 증가하고 있다. 모바일/웨어러블 기기를 통해 수집 가능한 라이프로그 데이터의 종류는 크게 개인의 신체활동 (예. 걸음 수, 수면 패턴), 생체 데이터 (예. 심박 수, 산소 포화도), 생활 습관 (예. 활동량, GPS, 전화 사용 시간 및 빈도, 앱 사용 종류 및 사용 패턴) 등이 있다.

라이프로그 데이터는 모바일/웨어러블 기기 기반 지속적인 센싱을 통하여 상시 데이터 수집이 가능하며, 다양한 센서 데이터 수집을 통한 새로운 형태의 데이터 확보가 가능하다는 측면에서 그 범위나 양이 방대하다는 특징으로 인해 개인의 생활 양식과 건강 정보를 유추하는 데 중요한 정보원으로 대두되고 있다. 그러나 이러한 데이터는 통계 기반 기계학습 또는 통계 처리를 통해 사용자의 전반적인 감정 및 정신상태 (예. 스트레스 및 우울감) 을 비롯하여 사용자의 일상생활 컨텍스트 (예. 생활 패턴, 방문 장소 등) 와 같은 개인 민감정보 유추가 가능하기에 사용자 개인정보에 위협을 가할 수 있으며, 추후 사용자의 일상생활에 피해를 입힐 수 있다는 단점이 있다 (예. 보험가입 차별, 사회적 낙인 등).

그러나 최근 시행된 유럽의 GDPR (General Data Protection Law) 및 국내에서 시행된 '데이터 3법'과 같은 데이터 보호 관련 법체계에 따르면 일상생활에서 모바일 및 웨어러블 기기에 내장된 센서를 통해 수집되는 개인 의 라이프로그 데이터 (예. 위치 정보, 활동 타입, 수면 상태 등)에 대한 구체적인 보호방침 및 수집되는 데이터 유형에 대한 명시는 부재한 것으로 보인다. 또한 모바일/웨어러블 센서를 통해 수집되는 데이터는 그 범위가 방대하고 기술적인 내용이 많아 배경지식이 없는 사용자가 주도적으로 데이터 수집에 동의하고 개인의 데이터를 관리하는 데는 어려움이 있어 보인다.

표1. 선정된 다섯 개 앱의 개인정보보호방침 별 GDPR 요구 항목 제공 여부

| | Samsung Health | Google Fit | Nike Run Club | Fitbit | Runday |
|---|---|---|---|---|---|
| 정의 | O | O | X | X | X |
| 개인정보의 수집 및 이용 | O | O | O | O | O |
| 사용되는 데이터 | O | O | O | O | O |
| 개인정보의 사용여부 및 목적 | O | O | O | O | O |
| 데이터의 전달 | O | O | O | O | O |
| (사용자의 동의 하) 데이터 공유 | O | O | O | O | O |
| 보안 | O | O | O | O | O |
| GDPR 준수 | X | X | X | O | X |
| 개인정보보호 방침의 변화 | O | O | O | O | X |
| 연락처 | O | O | O | O | O |

이러한 배경을 바탕으로 본 연구에서는 모바일/웨어러블 센서 데이터의 종류, 수집, 목적, 응용에 대하여 일반 사용자에게 쉽게 설명해주는 친숙한 가이드를 제공하여 사용자가 능동적으로 개인정보를 관리할 수 있도록 돕는 시스템 파일럿 디자인 연구를 수행하고자 하였다.

해당 연구 수행에 앞서 본 연구는 다음의 연구 질문을 설정하였다.

연구 질문 1. 현재 상용 센서 기반 어플리케이션의 개인정보보호방침 제공 방식은 어떠하며, GDPR이 권고하는 개인정보 보호 방침 관련 요구사항 부합 여부는 어떠한가?

연구 질문 2. 사용자가 주도적으로 센서 데이터 수집에 동의하고 이해하기 쉽도록 지원할 수 있는 사용자 친화적 시스템 디자인 방안은 어떤 것이 있을까?

우리는 센서 기반 상용 모바일 어플리케이션 기반 사전 조사 및 사용자 설문조사, 시스템 디자인 프로토타이핑 등을 통하여 현재 센서 기반 어플리케이션의 개인정보보호방침 제공 방식 현황 및 사용자 친화적 데이터 수집 시스템 디자인을 위한 사용자 요구사항 등에 대하여 도출할 수 있었다.

우리는 이 연구를 통해 현재 모바일/웨어러블 센서 기반 앱의 개인정보보호방침의 현황 및 한계점을 조사하고, 이를 바탕으로 사용자 친화적인 데이터 수집 시스템 디자인을 위한 도움을 줄 수 있을 것으로 기대한다.

## 2. 연구 수행

본 연구에서는 센서 기반의 모바일 어플리케이션 서비스의 개인정보보호 방침 및 서비스 이용약관의 현재 상태에 대하여 조사하였다. 해당 서비스의 개인정보보호 방침의 객관적 평가를 위해 평가기준으로 GDPR에서 요구하는 개인정보보호방침 항목의 제공여부 및 사용 프라이버시 관련 추가적인 평가사항을 선정하였다. 이와 더불어 현재 해당 서비스들의 개인정보보호 방침 제공 방식이 사용자 중심적인지 알아보기 위해 해당 서비스들의 개인정보보호방침 제공 측면에서의 UX/UI를 평가하였다. 언급된 두 가지 사전 조사를 통해 얻은 결과를 토대로 본 연구는 사용자 친화적인 개인정보 보호방침 알림 시스템의 프로토타입을 디자인했다.

### 2-1. 연구 ㅣ - 연구 방법

본 연구에서는 센서 기반의 신체 건강 모바일 어플리케이션을 대상으로 개인정보 보호방침의 제공 방식과 내용을 평가했다. 객관적인 평가를 하기 위해 본 연구는 첫번째 평가 기준으로 GDPR에서 요구하는 개인정보 보호방침 항목의 제시 여부를 확인하였다. GDPR에서는 다음의 항목을 개인정보 보호방침에 제시하는 것을 장려한다; 개인정보 보호방침 관련 용어 정의, 개인정보 수집 및 사용 여부, 사용 데이터 공개 여부, 개인정보 사용 여부 및 사용 이유, 정보의 전달 여부, 사용자의 동의 하 정보 전달 여부, 개인정보 보호 방식 설명, GDPR의 준칙에 맞게 작성되었는지 여부, 개인정보보호방침 변화 발생 시 명시 여부, 문의 가능 연락처. 본 연구에서는 센서 기반 신체 건강 모바일 어플리케이션 중 가장 대표적인 앱 5 가지 (Samsung Health, Google Fit, Nike Run Club, Fitbit, Runday)를 선정해 각 앱의 개인정보보호 방침을 조사해, GDPR에서 요구하는 프라이버시 요구 관련 사항의 충족 여부를 조사하였다. .

GDPR에서 요구하는 항목 이외에도 본 연구는 추가적인 평가 기준을 조사하였다. 그 기준은 다음과 같다. 개인정보보호 방침 제공 여부, 수집 데이터 저장 여부 및 저장 장소, 수집 데이터 삭제 가능 여부 수집 데이터 익명화 가능 여부, 사용자 주도의 공유 데이터 선정 가능 여부 등이 있다. 서비스 이용약관과 개인정보보호 방침과 모순되는 점이 있는지, 그리고 각 앱의 UX 및 UI를 조사하여 개인정보보호 방침의 제공 방식과 접근성 등을 확인했다.

그림 1. 사용자 친화적 프라이버시 정책 알림 시스템 디자인

### 2-2. 연구 ㅣ - 연구 결과

#### 2-2-1. 개인정보보호방침 조사 결과

[표 1]은 선정된 다섯 개 앱의 개인정보 보호방침별 GDPR 요구 항목 제공 여부를 보여주는 표이다. 조사 결과 선정 앱들은 대체적으로 GDPR에서 요구하는 항목을 개인정보 보호방침에서 제공하고 있는 것으로 확인되었다. 특히 개인정보 수집 이유 및 사용처, 수집 데이터 3차 제공 여부, 수집 데이터 보호 방식에 대한 구체적인 설명 제공의 경우 다섯 개의 앱 공통적으로 명시를 하고 있음을 확인 할 수 있었다. 하지만, 사용자로부터 수집한 센서 데이터를 어떻게 수집했는지, 그리고 어떻게 쓸것인지에 대해 구체적으로 설명된 바가 없다는 것도 알 수 있었다. 대부분의 경우, 사용자가 공유할 데이터를 스스로 정할 수 있는 기능이 없었으며, 있더라도 기본적으로 수집하는 정보를 미리 정해 놓았으며 사용자에게 알리지 않았다.

#### 2-2-2. UX/UI 조사 결과

Andow et al(2019)에서는 각종 서비스의 개인정보 보호방침을 분석한 결과, 글로 매우 길게 쓰여져 있었으며, 전문가조차 이해하기 난해한 표현이 많았다는 것을 알게 되었다고 한다 [1]. 본 연구에서도 각 앱의 개인정보보호 방침을 작성한 방식을 확인해본 결과, 대부분 글을 중심으로 항목별로 구체적인 설명을 했으며 사용자가 모두 읽기에는 양이 너무 방대했다. 하지만, Google Fit 같은 경우, 사용자가 이해하기 쉽도록 글과 그림, 동영상을 적극적으로 활용했다.

### 2-3. 연구 II - 연구 방법

본 연구는 서비스의 개인정보 보호방침을 확인하고 싶은 사용자 또는 연구자들을 대상으로 시스템을 디자인했다. 본 연구는 타겟 사용자를 상용 센서 기반 앱과 연동서비스를 제공하는 개발자, 프라이버시와 관련된 분야의 연구자, 그리고 서비스의 개인정보 처리 과정에 관심이 있는 사용자와 같이 개인정보보호 방침을 확인하고 싶은 사람들로 선정한 뒤, 시스템을 디자인 했다. 사용자가 손쉽게 확인하고 싶은 내용을 제공하는 것이 목적이기에, 연구는 개인정보 보호 방침과 방침에서 명시하고 있는 특정 내용을 앱별로 사용자가 자유롭게 찾아볼 수 있는 시스템을 구상했다.

본 연구는 시스템의 구상에 앞서 사용자에게 제공할 정보의 항목을 앞서 조사한 내용을 기반으로 정했다. 항목은 데이터 수집 여부 및 종류(Data Collection), 데이터 사용 공개 여부 및 방법(Data Usage), 데이터 수집 목적(Collection Purpose), 개인정보 전달(Data Transfer), 사용자의 동의 하 개인정보 공유(Data Disclosure), 데이터 처리 여부 및 방법(Data Processing), 그리고 보안(Security Measures)으로 정했다.

시스템 디자인은 UI 디자인의 대표적인 툴인 figma를 이용하여 그림1. 처럼 웹 기반 시스템을 디자인했다. 시스템은 하나의 행에 앱과 개인정보보호 방침, 그리고 우리가 정한 항목을 포함하는지 여부를 확인할 수 있게 하였다. 예를 들어 그림 1.의 index1에 해당하는 행에는 Nike Run Club의 개인정보보호 방침을 열람할 수 있는 버튼이 있으며, 연구에서 정한 항목별로 개인정보 보호 방침이 제공된 경우 O, 제공되지 않은 경우면 X로 표시했다.

사용자가 더 구체적인 정보를 보고 싶어하는 경우, O를 누르게 되면 개인정보보호 방침에서 해당 항목에 대한 내용을 간략하게 정리된 설명을 볼 수 있다. 예를 들어 그림1. 의 Samsung Health 행의 Data Collection 항목에 해당하는 O 표시를 누르게 된다면, 다음의 예시와 같은 센서 데이터 수집 사항에 대한 설명이 제공된다: 가속센서로부터 얻은 움직임 데이터

- 사진, 음성, 연락처 그리고 일정 정보
- 심장박동, 위치 정보와 같은 센서 데이터 (더보기)

사용자는 그림1.의 Filter 기능을 이용하여 자신이 원하는 앱만 열람 할 수 있다. Filter는 연구에서 정한 항목 중 사용자가 보고 싶은 항목을 선택할 수 있게끔 한다. 사용자가 Filter를 통해 보고 싶은 항목을 선택한 후, 시스템은 해당 항목을 개인정보 보호방침에서 제공한 앱만 보여준다.

### 2-4. 연구 II - 연구 결과

본 연구는 제시된 프로토타입을 바탕으로 사용자 대상으로 해당 프로토타입 디자인에 대한 인터뷰 기반 파일럿 스터디를 수행하였다 (몇 명 대상). 결과, “서비스를 이용하는데 있어서 궁금한 부분을 필터로 바로바로 찾을 수 있어 편해요. [...] 하지만 일반적인 서비스 사용자가 이 시스템을 굳이 이용하지 않을 것 같아요”의 반응이 있었다(참여자 1). 시스템의 유용성에 대한 측면 이외에도 디자인에 대한 피드백 또한 있었다. 현재 시스템은 연구가 정한 어플리케이션 의 개인정보 보호 방침에서 연구가 정한 항목들만 요약해서 보여준다. 이와 반대로 연구가 제시한 앱 이외에 사용자가 보고 싶어 하는 어플리케이션에서 사용자가 보고 싶어하는 개인정보 보호 방침의 내용 또는 서비스 이용 수칙에 대한 내용을 사용자가 자유롭게 검색을 할 수 있게 했으면 좋겠다는 의견이 제시되었다. 인터뷰 결과 “서비스가 민감도를 정량화 할 수 있었으면 좋겠어요. [...] 사용자가 한 눈에 자신이 사용하는 서비스가 얼마나 안전한지를 알 수 있으면 좋을 것 같아요.”라는 의견도 있었다 (참여자 3). 연구에서 정한 항목마다 민감도를 인터뷰 등 을 통해서 정량적으로 측정한 후, 측정한 민감도를 기반으로 각 어플리케이션이 얼마나 보안적으로 민감한지 수치로 표현을 하게 된다면 사용자가 개인정보보호 방침의 구체적인 내용을 보지 않게 되더라도 자신의 개인정보가 얼마나 잘 보호되고 있는지 알 수 있기 때문이다.

## 3. 결론 및 논의 사항

본 연구는 모바일/웨어러블 기반 센서 활용 앱의 개인정보 보호방침의 현재 상태가 어떤지, 그리고 GDPR이 권고하는 프라이버시 요구사항에 얼마나 충실한지를 알아보고자 다섯 개의 앱을 선정해 각 앱의 개인정보 보호 방침을 조사했다. 조사 결과 개인정보보호 방침은 대부분 GDPR이 권고하는 프라이버시 요구사항에 충실했으나, 수집하는 사용자의 센서 데이터에 대한 설명이 부족했으며, 개인정보 보호 방침의 제시 방식이 사용자가 이해하기 어렵게 작성되었다는 것을 알 수 있었다. 본 연구는 조사한 결과를 토대로 사용자 친화적 모바일/웨어러블 센서 데이터 수집을 위한 시스템 디자인 요구사항 및 개선사항에 대한 피드백을 정리하였다. 해당 연구 결과는 사용자가 능동적 개인정보 관리를 할 수 있도록 돕는 지능형 시스템 디자인 등의 추후 연구에 도움이 될 것으로 보인다

## 4. 참고문헌

[1] Benjamin Andow et al. (2019). PolicyLint: Investigating Internal Privacy Policy
Contradictions on Google Play. Santa Clara, CA, USA: 28th USENIX Security Smyposium. https://www.usenix.org/system/files/sec19-andow.pdf