30 בנובמבר 2021
כ״ו בכסלו תשפ״ב

המלצות להתנהלות הציבור בשימוש במכשירים לבישים למטרות ספורט ובריאות

רקע

בשנים האחרונות, עם התקדמות הטכנולוגיה והזמינות הנרחבת של שירותי רשת האינטרנט, מתגבר ומתפתח השימוש במכשירים חכמים ומכשירי האינטרנט של הדברים (IoT – Internet of Things). מכשירים לבישים הם קבוצה של מכשירי IoT שניתן ללבוש אותם על הגוף והם זמינים בתצורה של צמידים, שעונים חכמים, משקפיים, מכשירים הניתנים ללבישה על הראש וכו׳. למכשירים אלו השלכות על תחומי הבריאות, הרפואה, ספורט, תחבורה, פיננסים, משחקים, מוזיקה ועוד. **המכשירים אוספים מידע אישי רב ובעלי פוטנציאל גבוה לפגיעה בפרטיות המשתמשים.**[1]

מסמך זה מתמקד במכשירים לבישים למטרות ספורט ובריאות, שהם אחת התצורות הנפוצות ביותר של מכשירים לבישים.[2] **מטרת המסמך היא להציב זרקור על התופעה, לסקור את דרישות הדין ולהציע המלצות להתנהלות נכונה לשם צמצום הפגיעה בפרטיות המשתמשים.** יובהר כי המסמך אינו מבקש למנוע את השימוש במכשירים לבישים בתחום הספורט והבריאות, אלא לתת כלים להתנהלות נכונה של המשתמשים.

איסוף נתונים אישיים למטרות ספורט ובריאות

מכשירים לבישים למטרות ספורט ובריאות מתבססים, בין היתר, על איסוף נתונים על אודות המשתמש, לשם הפעלתם בצורה מיטבית. ישנם שני סוגים של איסוף נתונים למטרות ספורט ובריאות: נתונים הנאספים באופן אוטומטי באמצעות חיישנים או נתונים הנאספים על ידי הזנה ידנית על ידי המשתמש.

להלן מגוון נתונים הנאספים ממכשירים לבישים והדרך בה אוספים אותם: מיקום – נאסף באמצעות GPS – מערכת מיקום גלובלית; איכות האוויר שמסביב למכשיר – באמצעות חיישן ניטור איכות סביבה; אוכל שנצרך – מוזן ידנית; פעילות/תנועות ודפוסי שינה – חיישני תאוצה, צעדים וגובה; תפקוד ותיאום שרירים – חיישני לחץ; מוליכות עור כתוצאה מהזעה כמוקד לעוררות רגשית - חיישן GSR - תגובת עור גלוונית[3]; טמפרטורה ופריון – חיישן חום ואלקטרוגרפיה; דופק,

---

[1] ישנם סוגים חדשים של גופים שאוספים, משתפים ומשתמשים במידע בריאות ממכשירים לבישים לספורט ובריאות ואינם מוסדרים על ידי חוקים או תקנות של משרד הבריאות בנוגע לציוד רפואי וכן יותר ויותר מידע בריאותי נאסף, משותף או נעשה בו שימוש על ידי סוגים חדשים של ארגונים מעבר לארגוני הבריאות המסורתיים כפי שקורה בארה״ב כאשר גופים מסוג זה אינם מוסדרים תחת ה- HIPAA.

[2] שוק הטכנולוגיה הלבישה גדל מ-84 מיליון יחידות בשנת 2015 ל-245 מיליון יחידות בשנת 2019. ההכנסות בשוק הטכנולוגיה הלבישה מסתכמות ב-15 מיליארד דולר בשנת 2020. ההכנסות צפויות להציג קצב צמיחה שנתי (CAGR 2020-2024) של 3.8%, וכתוצאה מכך נפח שוק של כ-17 מיליארד דולר עד 2024. מרבית ההכנסות נוצרות בסין (4.8 מיליארד דולר בשנת 2020), גידול זה מראה על מגמת השימוש הנפוץ של מכשירים אלו.

מקור

מקור

[3] תגובת עור גַּלְוָנִית, הינה שינוי במוליכות העור הקשורה לתהליכים פיזיולוגיים ופסיכולוגיים המתרחשים בגוף. מקור

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

לחץ דם ודם חמצן – חיישני דופק, אלקטרו-קרדיוגרמות, אוקסימטרים; ומדידת תפקודים קוגניטיביים ופעילות מוחית – חיישנים לבישים על הראש.

הנתונים שנאספו מועברים באופן מקוון ליישום סלולרי או למסד נתונים אחר. נתונים אלו נשמרים בחוות שרתים מרוחקת (ענן) או במערכות מבוזרות בהן ניתן לנתח נתונים אלו ולהציג שינויים לאורך זמן.

בהנגשת הנתונים ותהליך איגומם ישנם יתרונות רבים למשתמשים, שכן באמצעות כלי השירות ומערכות בינה מלאכותית, יכול המשתמש לשמור על בריאותו ולהביא לשיפורה. יחד עם זאת, בתהליך זה גלומים אתגרי פרטיות חדשים עבור המשתמשים, שכן נתונים נוספים אלו על אודות המשתמש הינם בעלי ערך רב עבור גופים רבים, וישנו חשש שימוש לרעה במידע על ידם.

<u>סיווג מכשירים לבישים לספורט ובריאות</u>

מכשירים לבישים לספורט ובריאות ניתן לסווג לשלוש קטגוריות מרכזיות:

<u>שעונים חכמים</u>

שעונים חכמים הם מכשירים ממוחשבים או מחשבים קטנים המיועדים ללבישה על פרק כף היד, ויש להם פונקציונליות מורחבת ביחס לשעונים רגילים, הנובעת לרוב מתקשורת עם הטלפון הנייד. מרבית דגמי השעונים החכמים הנוכחיים מבוססים על מערכת הפעלה ניידת. חלקם פועלים כמכשירים מותאמים לטלפונים חכמים, ומספקים מסך נוסף בו ניתן ליידע את המשתמש על התראות חדשות, כגון הודעות שהתקבלו, שיחות או תזכורות ליומן. היצרנים ממשיכים לפתח את מוצריהם ולהוסיף תכונות, כגון מסגרות עמידות למים, מערכות ניווט גלובליות (GPS) ותכונות מעקב אחר כושר/בריאות. בתוספת חיישני אינרציה אמינים ורגישים עליהם, ניתן להשתמש כעת בשעונים חכמים כדי ללכוד ולנתח תנועות ידיים, כגון עישון או פעילויות אחרות.

<u>צמידי כושר</u>

צמידי כושר, המכונים גם מנטרי פעילות, נלבשים בדרך כלל על פרק כף היד, על החזה או על האוזניים, ונועדו לפקח ולעקוב אחר פעילויות ספורט בחוץ ולמדוד מדדים הקשורים לכושר גופני, כגון מהירות ומרחק הריצה, נשיפה, דופק והרגלי השינה. קבוצות כדורגל מקצועיות באירופה ובארצות הברית השתמשו במעקב הפעילויות בכדי לכמת את הביצועים הפיזיים של שחקנים.

<u>ביגוד חכם</u>

למרות שהיבטים של ביגוד חכם דומים לסוגים אחרים של מכשירים לבישים העוקבים אחר מצבו הגופני של הלובש, הם כוללים רשימה רחבה של מוצרים לבישים, החל מביגוד ספורטיבי, חליפות גוף ורצועות חזה וכלה בגרביים, מכנסי יוגה, נעליים, קסדות וכובעים עם מגוון רחב של חיישנים ותכונות.[4]

[4] מכשירים חכמים לבישים משכו את תשומת ליבם של ארגוני ספורט מקצועני בגולף, כדורגל, אתלטיקה, ריצה, כדורסל ובייסבול. קבוצות ספורט עושות שימוש במכשירים אלו לניטור המצב הגופני של השחקנים במהלך האימון, על מנת להפחית את מספר הפציעות ולהגביר את ביצועי הקבוצה. מכשירים אלו ניתן לסווג גם על פי היישום שלהם: ניטור ביצועים פיזיים ובטיחות: ניטור אחר תנועה ופוזיציה, ניטור פגיעה מהתנגשות, ניטור ביומכאני (תנועת חלקים

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

לרובם של האמצעים הלבישים קיימת אפליקציה תואמת, אשר קולטת את הנתונים המשודרים אליה מהאמצעי הלביש. מסמך זה מתמקד במכשירים עצמם.

מידע רפואי – סקירה משפטית

חוק הגנת הפרטיות והתקנות שהותקנו מכוחו מעניקים הגנה מוגברת על מידע רפואי. סעיף 7 לחוק קובע כי נתונים על מצבו הרפואי של אדם מוגדרים כ"מידע רגיש". לאור האמור, ובהתאם להוראת סעיף 8 לחוק, גוף אשר אוסף מידע רפואי על אדם, חייב ברישום המאגר בהתאם להוראות סעיף 8 לחוק.

כמו כן, על-פי התוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'התקנות' או 'תקנות אבטחת מידע'), מאגר מידע הכולל מידע רפואי מחויב ברמת אבטחה בינונית ומעלה. על-פי התקנות, מידת רגישותו של המידע השמור במאגר מהווה קריטריון ביחס לאופן יישום היבטים שונים של אבטחת מידע, כגון אופן ההתמודדות עם אירועי אבטחת מידע והאבטחה הפיזית והסביבתית של מאגר המידע.

הסיכונים לפרטיות

ככלל, השימוש הנפוץ במכשירים לבישים נובע מיעילותם וזמינותם של אמצעים אלו. עם זאת, שימוש זה עלול להביא למצב בו מידע רפואי הנשמר במאגרי המידע של החברות המפעילות את המכשיר, יזלוג מהמכשיר או שייעשה בו שימוש חורג על ידי צד שלישי. כל האמור מהווה סיכון לפרטיות וזאת במספר היבטים מרכזיים:

א. פרצות אבטחה:

ישנם שלושה אזורי אבטחה פגיעים הקשורים לאיסוף נתונים רפואיים ממכשירים לבישים. איומים אלה קשורים **לאדם** המשתמש במכשיר הלביש; **לנתונים במעבר** בין המכשיר לתוכנה; **ולאחסון הנתונים** המצטברים בבסיס נתונים, לאחר שהמידע עבר מהמכשיר לאחסון:

האדם המשתמש במכשיר הלביש

המשתמש עלול לאבד את המכשיר, בין אם באופן תמים או כתוצאה מאירוע גניבה, כך שללא אמצעי הגנה נוסף, יתאפשר לאדם שאינו מורשה, לגשת למידע רפואי רגיש המאוחסן במכשיר.

בעוד שהבעלים של המכשיר אחראי לשמירה על פרטיותו במכשיר שברשותו, מספר מחקרים מצאו[5] כי לחלק מהמשתמשים חסר הידע הטכני ליישום אמצעי אבטחה במכשירים לבישים.

בגוף). ניטור מצב פיזיולוגי לייעול ביצועים: קצב לב וניטור אלקטרוקרדיולוגי, סטורציית חמצן בשרירי, ניטור איכות שינה. שיקום וחזרה לאחר פציעה: ניתוח מוכנות רפואית לחזרה לפעילות ספורטיבית, ניתוח סיכונים לפציעה חוזרת.

[5] Crossler, R.E., & Bélanger, F. (2017). The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors. HICSS. למקור
Torre, I., Sanchez, O., Koceva, F. et al. Supporting users to take informed decisions on privacy settings of personal devices. Pers Ubiquit Comput 22, 345–364 (2018). למקור
למקור

כמו כן, למכשירים לבישים יש מסך קטן יותר בהשוואה למחשבים ולטלפונים חכמים, עובדה המקשה על הניווט והקריאה.

נתונים במעבר מהמכשיר הלביש

כאשר נתונים נמצאים במעבר, הם עשויים להיות חשופים להאזנות, כמו Sniffing (תהליך ניטור ולכידת כל החבילות העוברות ברשת נתונה) או Tapping (התקן חומרה המשמש לגישה לנתונים הזורמים ברשת מחשבים), וכן לשינוי או ניתוח התעבורה. דוגמא נוספת הינה האזנת סתר – יירוט בזמן אמת של תקשורת פרטית. התקפות אלו מהוות איום משמעותי כלפי מערכות לבישות, שכן הן יכולות לחשוף את המידע האישי של המשתמש בפני תוקף.
מכיוון שהעברת נתונים בין מכשירים לבישים מתבצעת, בדרך כלל, באמצעות טכנולוגיות אלחוטיות או בלוטות', הנתונים עלולים להימצא גם בסכנת שינוי, כך שהנתונים יהיו שגויים או לא שלמים.
דוגמא נוספת הינה התקפות ניתוח תעבורה - תהליך של מעקב אחר תנועת מידע המוחלפת בין מכשירים לבישים לטלפון חכם או לתוכנה, ממנה ניתן להסיק מסקנות מדפוסי התקשורת כדי לעקוב אחר משתמשים, לזהות את פעילותם או לזהות את המשתמש. האקרים, שהפכו לגורם המוביל בתחום ההפרות הנוגעות לנתוני ספורט ובריאות, עלולים לנסות להשתמש בנתונים כדי לגנוב את זהות המשתמש.
לאחר שמירת הנתונים וניתוחם בתוכנה, נתונים אלה עשויים להיות פגיעים לתוכנות זדוניות, כגון וירוסים, האקרים או כלי שיתוף קבצים.

נתונים באחסון לאחר העברת המידע מהמכשיר הלביש

בדרך כלל, הנתונים שנאספים באמצעות מכשיר לביש נשמרים על ידי החברה המפעילה במרכזי נתונים או על שרת ענן, שיש בהם פוטנציאל לחשוף את כל המידע על המשתמשים בעת פרצת אבטחה וזליגת המידע.[6]

ב. גישה של צד שלישי לנתונים המופקים ממכשירי בריאות לבישים:

המיזוג בין שיווק מכשירים לבישים לצרכי ספורט ובריאות, לבין שיווק דיגיטלי, יצר סוגי חדש של איסוף נתונים ושיטות שיווק דיגיטליות הנמצאים כיום בשימוש על ידי משווקי בריאות וחברות תרופות, המפותחות לשימוש בשוק המכשירים הלבישים.[7]

לאור האפשרות הקיימת כיום לבצע ניתוח נתוני עתק (Big Data), גם נתונים שאינם מוגדרים כנתונים רפואיים או רגישים, עשויים לשמש עבור הסקת מסקנות בנוגע למשתמשים. על כן, מעבר לפגיעה בפרטיות ובאוטונומיה האישית של המשתמשים, עלולות להיות לכך השלכות

[6] Kapoor, Vidhi and Singh, Rishabh and Reddy, Rishabh and Churi, Prathamesh, Privacy Issues in Wearable Technology: An Intrinsic Review (April 2, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020, Available at SSRN: למקור or למקור

[7] החשש הוא שמידע רגיש יועבר לצדדים שלישיים על ידי החברות המפעילות, מבלי שניתנה לכך הסכמת המשתמש. חשש נוסף הוא שייעשה שימוש חורג במידע על ידי בעל מאגר המידע עצמו, מעבר למטרה שלשמה נמסר המידע. לאור העובדה שחלק מן המידע שעשוי להיאסף הוא מידע רגיש ממנו ניתן ללמוד על מצבו הרפואי של המשתמש, כמו גם על אורחות חייו. העברתו לידי גורמים שלישיים, כמו למשל מעסיקים או חברות ביטוח, עלולה לפגוע בפרטיותו של המשתמש.

משמעותיות. לדוגמא, חברות ביטוח עשויות להעלות את פרמיית ביטוח הבריאות של המשתמש, בהסתמך על נתוניו הרפואיים כפי שנאספו באמצעות המכשיר הלביש.

המלצות שימוש במכשירים לבישים למטרות ספורט ובריאות

להלן יוצגו המלצות הרשות להגנת הפרטיות בנושא שימוש במכשירים לבישים למרות ספורט ובריאות. ההבהרות וההמלצות מבוססות, בין היתר, על העקרונות והכללים שהוצגו קודם לכן.

איתור הגדרות הפרטיות במספר מיקומים

אין זה מספיק לבדוק את הגדרות הפרטיות במכשיר עצמו. לרוב במכשירים לבישים, הגדרות הפרטיות יופיעו בשלושה מקומות: במכשיר עצמו, באפליקציה המקושרת למכשיר בטלפון שלכם וכל פורטל אינטרנטי שעשוי להיות מקושר לשירות. כמו כן, מומלץ לבדוק את ההגדרות בכל פלטפורמות מדיה חברתית או בעת יצירת חשבונות חדשים.

בדיקת הגדרות הפרטיות במכשיר הלביש

כאשר אנו מקבלים מכשיר חדש, הנטייה היא לעבור את תהליך ההתקנה במהירות המרבית, ולדלג על שלבים, כדי להתחיל להשתמש בו מיד. הרשות ממליצה להתעכב על כל שלבי ההתקנה, שכן **קבלת הגדרות ברירת המחדל לפרטיות במכשיר עלולה לפגוע בפרטיותכם**. למשל, חשוב לבדוק האם המכשיר אוסף ומשתף את הנתונים הסטטיסטיים והמיקומים שלכם. במקרים מסוימים מכשירים לבישים מחוברים לרשתות חברתיות. על כן שימו לב האם המכשיר משתף את הנתונים הרפואיים שלכם עם אחרים, משתף באופן ציבורי, משתף עם "חברים" בלבד, או שאינו משתף כלל. שקלו היטב האם לאפשר לאחרים לדעת את מסלול הריצה שלכם או את הזמנים שבהם אתם נמצאים במקומות מסוימים.

שקילת השבתת מעקב אחר מיקום

רוב המכשירים הלבישים מבצעים מעקב מיקום גאוגרפי, בין אם על המכשיר או על האפליקציה המשויכת למכשיר. הדרך הקלה ביותר להגן על עצמכם עשויה להיות פשוט לבטל מעקב אחר מיקום גיאוגרפי במכשיר. מידע על מיקום מדויק הוא רגיש, מחקרים מראים[8] שניתן להשתמש בו כגורם מזהה גבוה.

עיון במדיניות הפרטיות

מכשירים לבישים אוספים עלינו נתונים, מה שהופך אותם למועילים כל כך. מדיניות הפרטיות של כל מכשיר נדרשת לפרט מהם השימושים שתוכל החברה המפעילה לעשות בנתונים שלנו. חפשו נושאים אלה במדיניות הפרטיות של המכשיר הלביש, כדי שתוכלו לשקול את השימוש במכשיר.

[8] Alexandra-Mihaela Olteanu, Kévin Huguenin, Reza Shokri, Mathias Humbert, Jean-Pierre Hubaux. Quantifying Interdependent Privacy Risks with Location Data. IEEE Transactions on Mobile Computing, Institute of Electrical and Electronics Engineers, 2017, 16 (3), pp.829-842. ff10.1109/TMC.2016.2561281ff. ffhal-01266229v2f למקור

<u>פרואקטיביות בהגנה על המידע האישי שלכם</u>

מומלץ לקיים מדי פעם בדיקת עדכונים למדיניות הפרטיות של המכשיר הלביש ובדיקה קבועה של עדכון אבטחת המכשיר.

על מנת להקטין את איסוף המידע ניתן לבצע מספר פעולות:

- בחירת הגדרות פרטיות חזקות יאפשרו לצמצם את הנתונים הזמינים לגורמים נוספים.
- כיבוי המכשיר – בעת שהמכשיר כבוי לא ייאסף מידע.
- מחיקת מידע לצמיתות – אם אינכם זקוקים יותר למכשיר, ודאו שכל המידע האישי הוסר לצמיתות. שימו לב כי הדבר עשוי לכלול יותר מאשר איפוס מכשיר להגדרות היצרן.
- שיתוף מידע – אם בכוונתכם לשתף את המידע ברשתות חברתיות או בפורומים מקוונים של משתמשי המכשיר, יש לשים לב כי המידע יהיה נגיש לעיני אנשים רבים (בהתאם להגדרות הפרטיות שלכם ברשתות החברתיות), ולמעשה תאבדו שליטה על המידע.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב