הכנסת

מרכז המחקר והמידע

שמירתם של נתוני מיקום במכשירים סלולריים חכמים והשימוש בהם

מוגש לוועדת המדע והטכנולוגיה

כתיבה: רועי גולדשמידט

אישור: שרון סופר, ראש צוות

עריכה לשונית: מערכת "דברי הכנסת"

כ"ג בחשוון תשע"ב

20 בנובמבר 2011

הכנסת, מרכז המחקר והמידע

קריית בן-גוריון, ירושלים 91950

טל': 02 - 6408240/1

פקס: 02 - 6496103

www.knesset.gov.il/mmm

מסמך זה נכתב לקראת דיון בוועדת המדע והטכנולוגיה בהצעה לדיון מהיר של ח"כ איתן כבל בנושא: השימוש בנתוני מיקום במכשירי סלולר חכמים – פרטיות ושימושיות.

המסמך סוקר את נושא נתוני המיקום במכשיר הסלולרי: מגוון הטכנולוגיות, יישומים אפשריים שלהן, החשש לפגיעה בפרטיות בשל שימוש בנתונים אלה ועוד. המסמך אינו עוסק בהיבט המשפטי של השימוש בנתוני מיקום ובשימוש של רשויות המדינה בנתוני מיקום.[1]

במסמך מוצגות עדויות של מומחים בפני הסנאט של ארצות-הברית ועמדתה של קבוצת עבודה של האיחוד האירופי בנושא נתוני מיקום. כמו כן, מוצגות עמדת משרד התקשורת, חברת "פרטנר" וחברת "פלאפון" בסוגיה.[2] לא נתקבלה תשובה מחברת "סלקום".

1. חדירתם לשוק של מכשירי הטלפון הניידים

בסוף שנת 2010 היו בעולם כ-5.1 מיליארד מנויים על קו טלפון נייד – מספר נפשות שהוא כ-75% מאוכלוסיית העולם.[3]

על-פי נתוני הלשכה המרכזית לסטטיסטיקה, **ל-91% מבני 20 ומעלה בישראל יש טלפון נייד. מאלה שברשותם טלפון נייד, 18% גולשים באמצעותו באינטרנט ו-10% משתמשים באמצעותו בתוכנת ניווט (GPS).**[4]

על-פי נתוני סקר של OurMobilePlanet.com משנת 2011, בישראל שיעור החדירה לשוק של מכשירי סמארטפון[5] הוא כ-31%, והיא במקום ה-10 מ-30 המדינות הנסקרות. בראש הרשימה ניצבת סינגפור, שבה 62% חדירה לשוק של מכשירי סמארטפון.

מן הנתונים עולה כי הטלפון הנייד הפך למוצר צריכה בסיסי בחלק ניכר מהעולם בכלל ובישראל בפרט. **מחקרים מן השנים האחרונות מלמדים שעיקר הגידול בשימוש במחשב ובאינטרנט הוא בשימוש במכשירי טלפון חכמים (להלן, סמארטפונים) ובמכשירי טאבלט** (מחשבי לוח, דוגמת אייפד) ולא בשימוש במחשבים אישיים (דסקטופים).

הגידול במספרם של המשתמשים בסמארטפונים צפוי שיימשך ואף יתגבר, בשל התפתחות השוק והשירותים המוצעים בו והשינוי במעמדם של מוצרים ממוצרי יוקרה למוצרי צריכה כמעט בסיסיים. בעקבות שינוי זה מתרחשים כיום תהליכים של התאמת הגלישה באינטרנט למדיום השימוש החדש יחסית, המכשיר הסלולרי, ופיתוח של שלל יישומים – אפליקציות – למען המשתמשים במכשיר סלולרי.

---

[1] נושא השימוש של רשויות המדינה בנתוני מיקום מוסדר בעיקרו בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007.

[2] תשובת חברת "פלאפון" נתקבלה לאחר סיום כתיבת מסמך זה, ועודכנה לאחר הדיון בוועדת המדע והטכנולוגיה בנושא.

[3] Global Wireless Subscriptions Reach 5 Billion, September 17, 2010.

[4] הלשכה המרכזית לסטטיסטיקה, לקט נתונים מתוך הסקר החברתי 2010: שימוש במחשב ובאינטרנט, 17 בנובמבר 2011.

[5] סמארטפון הוגדר בסקר כך: טלפון נייד שיש לו מערכת הפעלה, מסך מגע, תצוגה מוגדלת או מקלדת מלאה. ראו אתר האינטרנט OurMobilePlanet.com, תאריך כניסה: 17 בנובמבר 2011.

2. נתוני מיקום ושירותים המבוססים על מיקום[6]

טכנולוגיות שונות מאפשרות זיהוי מיקום של מכשירי טלפון נייד: GPS, אנטנות סלולר, נקודות Wi-Fi (תקשורת אינטרנט אלחוטית) וכתובות IP (פרוטוקול אינטרנט) – כל אלה מאפשרים, בדרכים שונות, ליצור מעין מפה של האזור שבו מצוי המכשיר הנייד ולזהות את מיקומו.

עבור חברות הסלולר, זיהוי המיקום מאפשר לספק למשתמשים שימוש במכשירי הסלולר לשם שיחה, גלישה ועוד, במהירות. גם בסביבה שבה אי-אפשר לזהות מיקום באמצעות GPS (למשל בתוך מבנים), הטכנולוגיות האחרות מאפשרות לזהות את מיקום המשתמש באופן יעיל , הצורך פחות חשמל מהמכשיר, ומקצר את הזמן עד לקבלת השירות. ולכן לדידן הוא אמצעי טכנולוגי חשוב. כפי שיובהר להלן, נתוני מיקום מאפשרים לא רק מתן שירות רגיל אלא גם מתן שירותים המבוססים על מיקום ופרסום ממוקד.

בעוד בעבר חברות מיפו את נקודות ה-Wi-Fi באמצעות כלי-רכב שסרקו את האזור, כיום חברות עושות שימוש במכשירי הקצה של המשתמשים כדי לערוך מעין סריקה של נקודות Wi-Fi, ובאמצעות הצלבת מידע זה עם מידע על אנטנות סלולר ומידע המבוסס על GPS, הן מצליחות למפות את המרחב ולקבוע את מיקומם של המשתמשים.

הגידול בשימוש בסמארטפון ולצדו ההתפתחות הטכנולוגיות של זיהוי מיקום הובילו לפיתוחם של שירותים המבוססים על מיקום (Location Based Services). בהכללה, הכוונה לשימוש במידע על מיקומו של המשתמש כדי לספק לו שירות התואם את צרכיו ברגע הנתון. שירותי מפות ותחבורה, מערכות לחיפוש מסעדות, מקומות בילוי או "נקודות עניין", רשתות חברתיות ועוד עושים שימוש בנתוני המיקום של המשתמש (מיקום סמארטפון) כדי לספק לו את השירות המבוקש. **כפי שיובהר להלן, יישומים רבים נוספים, שזיקתם לנתוני מיקום אינה ברורה או הכרחית, אוספים גם הם מידע על מיקום המשתמש.**

מחד גיסא, שימוש בנתוני מיקום עשוי להניב תועלת למשתמש הקצה המעוניין במידע מדויק ככל האפשר התואם את הצרכים שלו במיקומו הנוכחי; מאידך גיסא, הוא עלול לגרור פגיעה חמורה בפרטיותו של המשתמש בשל איסוף מידע מקיף על מיקומו לאורך זמן.

בשל היחס הכמעט אינטימי של משתמשי הסלולר למכשיר (רוב הזמן המכשיר מצוי בקרבת המשתמש, והשימוש בו נעשה על-ידי אדם אחד מסוים ומכיל מידע אישי), איסוף של נתוני מיקום יכול ליצור מעין מפה של חייו של המשתמש: היכן הוא גר, היכן הוא עובד, מהו המסלול היומיומי שלו ועוד.

כמובן, שילוב מידע על מיקום עם מידע נוסף – למשל על שאילתות החיפוש של המשתמש במנוע חיפוש – יכול להוביל לפגיעה מוגברת בפרטיותו.

עבור חברות הטכנולוגיה השונות, למידע על המיקום יש לא רק ערך טכנולוגי – היכולת לשפר את השירות למשתמשים – אלא גם ערך פיננסי רב, בשל היכולת לזהות דפוסי שימוש והתנהגות וליצור פרסום מדויק ביותר לצרכנים מסוימים.

---

[6] ראו עדותו של אשקן סולטני בסנאט להלן, וכן שיחה עם עו"ד עמית אשכנזי, יועץ משפטי, הרשות למשפט ולטכנולוגיה, משרד המשפטים, 16 בנובמבר 2011.

3. הודעת "וריזון ווירלס" (Verizon Wireless)

"וריזון", חברת תקשורת אמריקנית גדולה, שבין השאר בבעלותה מפעילת סלולר וספקית אינטרנט, מפרסמת, מאוקטובר 2011, מכתב ללקוחותיה ובו פרטים על שינויים במדיניות הפרטיות שלה.[7]

על-פי המידע שפרסמה, "וריזון ווירלס", מפעילת הסלולר של "וריזון", החברה מפעילה "תוכניות פרסום חדשות" ובמסגרתן **ייעשה שימוש במידע שייאסף ממכשירי הסלולר, ובין השאר כתובות אתרים שאליהם גלש הלקוח; מלות חיפוש שהלקוח השתמש בהן; מיקום המכשיר הסלולרי; אפליקציות המותקנות על גבי המכשיר ודפוסי שימוש. נוסף על כך, ייאספו נתונים על שימוש במוצרים ובשירותים של "וריזון" וכן מידע דמוגרפי ומידע על תחומי עניין, המתקבל מחברות אחרות.**

מטרות איסוף המידע האמור, על-פי "וריזון": ליצור דוחות שוק ודוחות עסקיים עבור החברה ועבור גופים אחרים, ולספק פרסום רלוונטי יותר למשתמש הספציפי במכשיר הסלולר.

על-פי האמור במכתב, "החברה לא תחלוק עם חברות אחרות חוץ מ"וריזון" כל מידע שיזהה את המשתמש באופן אישי".

משתמש שאיננו מעוניין לחלוק את המידע האמור יכול לחסום את איסוף המידע באופן אקטיבי (Opt-Out). ללא חסימה זו, ברירת המחדל היא איסוף של המידע האמור.

שניים מחברי הקונגרס האמריקני, אדוארד מרקי וג'ו ברטון, העוסקים בנושא הפרטיות, שלחו ל"וריזון" מכתב בנושא זה וביקשו להבין את העילה לשינויים במדיניות החברה, את חוקיות המהלך ואת הפרקטיקות הנהוגות בתחום זה.[8]

הנקודה המהותית והעיקרית בתשובת "וריזון" היא כי **התפיסה של החברה היא שהשימוש שלה במידע על משתמשיה, לגבי הסלולר והאינטרנט בכלל, הוא לגיטימי, משום שהוא נאסף באופן אנונימי ומוגש כמידע מרוכז על אוכלוסיית משתמשים גדולה.** לטענת "וריזון", פרקטיקות איסוף המידע שלה אינן ייחודיות אלא מאפיינות את השוק שבו היא פועלת, וההבדל העיקרי בינה לחברות אחרות הוא בחשיפת המידע ללקוחותיה ומתן הסבר מפורט ואפשרות לחסום את איסוף המידע.[9]

"וריזון" היא, כאמור, חברה המפעילה שירותי תקשורת סלולרית, אך כפי שנראה להלן, נתוני מיקום נאספים ומצויים בשימוש בידי חברות נוספות: מפתחי אפליקציות, מפתחי מערכות הפעלה ועוד.

4. פרשיית "אפל"

[7] TechCrunch, Verizon Welcomes Users To The Opt-Out, Ad-Targeting Party, November 16, 2011, retrieved: November 17, 2011

[8] לעיון במכתב ראו: אתר האינטרנט של חבר הקונגרס מרקי.

[9] לעיון בתשובת "וריזון" ראו כאן.

באפריל 2011 פרסמו שני חוקרים בתחום המחשבים (אלסדיר אלן ופיט וורדן) כי מכשירי אייפד 3G ומכשירי אייפון של חברת "אפל" שומרים מידע על מיקום המשתמשים, כולל מידע על היסטוריית המיקומים שלהם, זמן רב מאוד.[10]

על-פי הפרסומים, מאז החלה "אפל" להשתמש במערכת ההפעלה IOS-4, החברה החלה לשמור מידע על מיקומו של המכשיר – הן על גבי המכשיר והן על גבי המחשב האישי בעת סנכרון של המכשיר הנייד עם מחשב. המידע נשמר, כך על-פי הפרסומים, בקובץ שאיננו מוצפן, והגישה אליו פשוטה יחסית הן למי שמחזיק במכשיר הנייד (אייפון או אייפד) והן למי שהמחשב הנייח המשמש לסנכרון נגיש לו.

במידע על המיקום האמור נכללים נתונים על מיקומן של רשתות Wi-Fi ("נקודות חמות") ואנטנות הסלולר הסמוכות ביותר למקומות שבהם שהה המכשיר (עד כ-100 מיקומים ביום), והוא נשמר זמן ממושך, עד שנה. החוקרים ציינו שקל יחסית להפוך את המידע למפה מפורטת המצביעה על כלל המקומות שבהם שהה המכשיר – ומטבע הדברים גם בעליו. **המידע האמור מועבר למכשיר חדש אם המשתמש מחליף מכשיר. יש לציין כי כפי הנראה, המידע במתכונת זו (שבה יש זיהוי של המשתמש) אינו נשלח לחברת "אפל", ופריצה אליו מרחוק היא תהליך מורכב.**

הכתבות שפורסמו על שמירת המידע על מיקומם של משתמשי "אפל" עוררו עניין בקרב הציבור והובילו לבחינה מורחבת של הנושא, הן על-ידי חוקרים והן על-ידי הממשל האמריקני.

לאחר עליית הנושא לכותרות התברר כי <u>שמירת נתוני המיקום של המשתמשים איננה נחלתה הבלעדית של חברת "אפל", וגם חברות אחרות ("גוגל", באמצעות מערכת ההפעלה אנדרואיד, "מיקרוסופט", באמצעות מערכת ההפעלה שלה וחברות רבות נוספות, ובהן מפעילות סלולר ומפתחות אפליקציות)</u>, שומרות מידע על מיקום משתמשים בדרכים דומות. למעשה, בעיות דומות קיימות בכל סמארטפון.

4.1. שימוע הסנאט האמריקני בנושא הגנה על הפרטיות במכשירים ניידים

בחודש מאי 2011 קיימה ועדת המשנה לנושאי פרטיות, טכנולוגיה ומשפט של הסנאט האמריקני שימוע בנושא הגנה על פרטיות במכשירים ניידים דוגמת מחשבי טאבלט וטלפונים חכמים. בשימוע הציגו את הנושא ואת עמדתם גופים שונים, ובהם החברות "אפל" ו"גוגל". להלן יוצגו נקודות עיקריות שהתבררו בשימוע:

4.1.1. עיקרי עדותו של היועץ והחוקר לענייני פרטיות אשקן סולטני (Ashkan Soltani) בפני ועדת המשנה של הסנאט[11]

10 O'reilly Radar, Got an iPhone or 3G iPad? Apple is recording your moves, by Alasdair Allan and Pete Warden, April 20, 2011. Retrieved: November 14, 2011.

11 Testimony of Ashkan Soltani, Independent Privacy Researcher and Consultant, hearing before **the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law**, on "Protecting

מידע על מיקום מצוי בידי גורמים מסוגים שונים ועל בסיס טכנולוגיות שונות. עם טכנולוגיות אלו נמנות GPS, איתור מיקום גיאוגרפי לפי אנטנות סלולר, איתור על-פי נקודות Wi-Fi, זיהוי על-פי כתובת אינטרנט (IP). עם הגורמים המחזיקים מידע על מיקום נמנים ספקי שירות סלולר; ספקי מידע על מיקום (location Providers) דוגמת "אפל", "גוגל ו"סקייהוק"; חברות נוספות שאוספות מידע על מיקום ומספקות אותו לגורמים אחרים, דוגמת אתרים, אפליקציות ומפרסמים.

חברות המספקות מידע על מיקום, דוגמת "גוגל", ערכו בעבר, על-פי פרסומים, מיפוי ואיסוף של מידע על מיקומן של נקודות Wi-Fi ואנטנות סלולר באמצעות כלי-רכב המצוידים בסנסורים, אך בהמשך החלו לעשות שימוש במידע המצוי במכשירים של משתמשי הקצה בסלולר כדי לאסוף מהם מידע על מיקומן של אנטנות סלולר ונקודות Wi-Fi. כעיקרון, משתמשי הקצה יכולים לבחור לבטל את אפשרות איסוף המידע האמור, אך איסופו הוא ברירת המחדל המאושרת על-ידי המשתמש כחלק מהגדרות השימוש במכשיר בעת התחלת השימוש. כדי לבטל את איסוף המידע יש צורך, לעתים קרובות, לקרוא הסבר טכני ארוך שאיננו ברור למשתמש הפשוט. **על-פי כתבה שפרסם "וול סטריט ג'ורנל" באפריל 2011, מכשירי אייפון של "אפל" המשיכו לשדר נתוני מיקום גם לאחר שנבחרה במכשיר האפשרות להפסיק את הפעולה.** כאמור לעיל, מהמידע שפרסמו וורדן ואלן עלה שהמידע נשמר גם על גבי המכשיר כקובץ Cache ואי-אפשר להפסיק את איסוף המידע על מיקום שנשמר על גבי המכשיר. בעקבות הפרסום האמור הכריזה "אפל" על "תיקון הבאג", המקטין את גודל קובץ מידע המיקום על המכשיר, מבטל את הסנכרון ומוחק את קובץ המיקום בעת הניתוק משירותי מיקום.

לא זו בלבד שהמידע מועבר לספקיות מיקום אלא שלעתים קרובות שימוש באפליקציות שמספקים גורמים אחרים (צד ג') דורש גם הוא נתוני מיקום. בדצמבר 2010 מצא "וול סטריט ג'ורנל" כי 47 מתוך 101 האפליקציות הפופולריות העבירו את נתוני מיקום הטלפון ו-56 מהאפליקציות הללו העבירו אמצעי זיהוי אחרים (מספר סדרתי של חומרה למשל). **יש לציין כי כיום יש אפליקציות שעושות שימוש במידע נוסף במכשיר, למשל כתובות, היסטוריית חיפוש, הודעות טקסט ועוד. אומנם יש אפליקציות שלגביהן ברור הצורך במידע על מיקום, אך משתמע כי חלק ניכר מהן אוספות מידע זה פשוט מפני שיש באפשרותן לעשות זאת.**

אשקן סולטני ציין בעדותו בפני הסנאט כי גם המידע על מיקום, שהוא אנונימי כביכול וחלק מן החברות מתרצות את השימוש בו בהיותו "מידע סטטיסטי", יכול לאפשר "זיהוי לאחור". לכן למעשה, רוב המידע האמור איננו אנונימי לגמרי. נוסף על כך, המידע על המיקום מדויק ברמה של 20–60 מטרים והאיסוף שלו מאפשר ליצור רצף מיקומים מפורט ומתמשך; לפיכך המידע הופך למידע רגיש, כזה שאפשר להצליב בקלות יחסית עם פרטי מידע נוספים. ספקי שירותים שונים נוטים להגדיר את שיתוף המידע על מיקום כברירת מחדל של השירות, ולהציע את שירותיהם בשיטת "הכול או לא כלום" – היינו, על המשתמש לחלוק את המידע באופן גורף או שלא יוכל להשתמש בשירות מסוים.

Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy", May 10, 2011. Retrieved: November 13, 2011.

סולטני מסיים את עדותו בכמה המלצות:

- **יש לספק ללקוח שקיפות רבה יותר אשר למידע הנאסף עליו: מהו, כיצד הוא נשמר, למי הוא מועבר, כיצד הוא מאובטח ולמה הוא משמש.**
- **יש הכרח להבחין בין שימוש אקטיבי לשימוש פסיבי במידע ובין שימוש של צד א' (החברה עצמה) לבין העברתו לידי צד ג'.**
- **על הספקים והמפתחים להבטיח כי המידע מאובטח ומנוהל בהתאם לציפיות המשתמשים.**
- **על הספקים והמפתחים להציע ללקוחות אפשרויות בחירה מגוונות (ולא רק "הכול או לא כלום"), כדי שהחלטותיהם יתאמו את צורכיהם ויובאו בחשבון שיקולי פרטיות.**

4.1.2. עיקרי עדותו של סגן הנשיא לטכנולוגיית תוכנה של חברת "אפל", ד"ר גאי טריבל (Guy Tribble), בפני ועדת המשנה של הסנאט[12]

חברת "אפל" אימצה מדיניות פרטיות מקיפה לכל מוצריה והטמיעה יישומים כדי להגן על המידע האישי של לקוחותיה. החברה גם מחויבת לספק את דרישת לקוחותיה לשירותים המבוססים על מיקום שהם מדויקים ומהירים. לשירותים אלו יתרונות רבים: נוחיות ובטיחות בביצוע קניות, טיולים ועוד. **לשם כך, החברה מספקת כלים קלים לשימוש ולשליטה לשם איסוף המידע והשימוש בו. החברה איננה חולקת מידע אישי המאפשר זיהוי המשתמש עם צד ג' למטרות שיווק של צד ג' ללא הסכמה של המשתמש. מפתחי אפליקציות נדרשים להתחייב להגבלות שונות המגינות על המשתמשים.** "אפל" איננה עוקבת אחר מיקומם של לקוחותיה, מעולם לא עשתה זאת ואין בכוונתה לעשות כך בעתיד.

טריבל הציג בפירוט את מדיניות הפרטיות של "אפל", שעיקרה הוא שאיסוף המידע נעשה באופן אנונימי שאיננו מאפשר זיהוי אישי כדי לספק ביעילות שירותים ומוצרים המבוססים על מיקום. עם זאת, לשם הפעלת חלק מן היישומים יש צורך במידע אישי. דוגמה לכך היא השירות "מצא את האייפון שלי".

ככלל, משתמע מעדותו של טריבל כי השימוש בשירותים המבוססים על מיקום מחייב גישה לפרטי המיקום של משתמש הקצה, אך המשתמש יכול למנוע את הגישה למידע זה באמצעות ויתור על שירותים המבוססים על מיקום ולחלופין למנוע חלק מהפצתו באמצעות חסימת הגישה של חלק מן האפליקציות למידע.

אשר לצד ג', לדוגמה מפתחי אפליקציות העושים שימוש בנתוני מיקום או בפרטי קשר, הדבר תלוי במדיניות הפרטיות של החברה המפתחת את האפליקציה.

נציג "אפל" ציין כי החברה החלה להציע שירותים המבוססים על מיקום בינואר 2008, בשלל מכשירים שלה. שירותים אלה מאפשרים למשל לקבל הנחיות הגעה לכתובת מסוימת או לחפש מסעדה באזור שבו המשתמש נמצא. המשתמש יכול לבחור לנטרל את כל השירותים המבוססים על מיקום במכשיר. כדי

[12] Testimony of Dr. Guy "Bud" Tribble, Vice President for Software Technology Apple Inc., hearing before **the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law**, on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy", May 10, 2011. Retrieved: November 13, 2011.

להשתמש באפליקציה המחייבת מידע על מיקום נדרשת הסכמתו של המשתמש בעת הפעלתה הראשונית של האפליקציה – לא ניתן להפעיל אפליקציה כזאת ללא מתן אישור.

אשר לשימוש של חברת "אפל" בנתוני מיקום של משתמשיה, החברה מתייחסת לכך כאל "מיקור המונים" (Crowd Sourcing), שמטרתו לאפשר למכשירים להגיב מהר ובאופן חסכוני ולאתר מיקום ללא צורך מתמיד בביצוע סריקה לשם כך אלא בהסתמך על ניסיון נצבר של המערכת לעניין מיקומן של "נקודות חמות" ואנטנות סלולר. מאגר המידע הכולל על האנטנות ו"הנקודות החמות" אינו חושף מידע אישי על שום לקוח.

טריבל ציין **כי בעבר היו מועברים פרטי מידע שונים, ובהם מידע על מיקום, בעת סנכרון עם תוכנת ה"איי-טיונס" על גבי מחשב** וכי בשל תקלה (באג) במערכת ההפעלה של "אפל", גם במקרים שהמשתמש היה חוסם את השימוש בשירותים המבוססים על מיקום היה המכשיר שולח מידע אנונימי על "נקודות חמות" ואנטנות סלולר באזור למאגר המידע של "אפל". תקלות אלה תוקנו בעדכון מערכת ההפעלה ב-4 במאי 2011. **יצוין כי המידע בעדותו של נציג "אפל" מפורט והובא לעיל בקצרה.**

4.1.3. עיקרי עדותו של אלן דוידסון (Alan Davidson) מנהל המדיניות הציבורית של חברת "גוגל" למדינות אמריקה בפני ועדת המשנה של הסנאט[13]

הגנה על פרטיות ואבטחה הן חיוניות למסחר באינטרנט. אמון הלקוחות הוא רכיב הכרחי בהצלחתם של המוצרים, ולכן כישלון של החברה להציע הגדרות ברורות, שקיפות ושליטה במידת הפרטיות של המשתמש, סופו לגרום לוויתור של משתמשים על שירותים של החברה, כפי שאכן קרה במקרה של שירות "גוגל באזז". שיתוף מידע על מיקום במכשירים תומכי אנדרואיד **(מערכת ההפעלה של "גוגל")** מחייב את הסכמתו של המשתמש באמצעות הודעה על אישור מצדו.

דייוידסון ציין בעדותו כי שירותים המבוססים על מיקום הם תחום מסחרי המצוי בצמיחה ויש להם ביקוש רב. לדוגמה, בשנה האחרונה כ-40% מהשימוש בשירות "גוגל מפות" היה ממכשירים ניידים. כיום אפליקציות המבוססות על מיקום הן לא רק מצרך מסחרי נפוץ אלא משמשות גם למטרות הצלה, למשל שליחת הודעות על ילדים נעדרים לכל הגורמים המפיצים את המידע לציבור, באזור שבו היתה ההיעלמות; התרעות על סופות מסוכנות באזורים מסוימים ועוד. **קיומן של אפליקציות אלה תלוי בקבלתם של נתוני מיקום.**

"גוגל" מייחסת חשיבות רבה לנושא הפרטיות והגדירה חמישה עקרונות מנחים בנושא: השימוש במידע נועד לספק למשתמשים מידע ושירותים בעלי ערך; פיתוח המוצרים ייעשה בהתאם לסטנדרטים גבוהים של פרטיות; יש ליצור שקיפות בתחום איסוף של מידע אישי ושימוש בו; יש לאפשר ללקוחות בחירה של ממש בתחום ההגנה על פרטיותם; יש לנהל באופן אחראי את המידע שהחברה מחזיקה.

[13] Testimony of Alan Davidson, Director of Public Policy, Google Inc., hearing before **the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law**, on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy", May 10, 2011. Retrieved: November 13, 2011.

לדברי נציג "גוגל", החברה איננה אוספת שום מידע על מיקום ללא הסכמה מפורשת של המשתמש לחלוק מידע זה: בהליך ההתקנה נדרשת על-ידי מערכת ההפעלה הסכמת המשתמש לאיסוף מידע אנונימי על מיקום. **גם לאחר אישור לחלוק את המידע בעת הגדרת המערכת, יכולים משתמשי "גוגל" לחסום את שיתוף המידע לעניין מיקום בקלות. אם משתמש מסכים לאיסוף מידע על מיקום,** המידע הנאסף על-ידי "גוגל" עובר תהליך אנונימיזציה. אין דרך לקשור אותו למשתמש מסוים ורובו נמחק כעבור כשבוע. **מידע מועט על מיקום של "נקודות חמות" ואנטנות סלולר, נשמר על גבי המכשיר כדי לאפשר מתן שירות מהיר, יעיל וחסכוני בסוללה.**

כדי לשרת לקוחות באזורים ללא קליטת GPS או במכשירים ללא שבב GPS, וכדי לספק שירות יעיל ומהיר יותר, "גוגל", כמו חברות אחרות, יצרה מאגר מידע המצליב נתונים על "נקודות חמות" ואנטנות סלולר. יצרניות המכשירים הסלולריים יכולות להתקין תוכנת זיהוי מיקום של "גוגל" במכשירים וכך לאפשר מידע על מיקומו של המכשיר. אך ברירת המחדל של ההפעלה בעת התקנת המערכת היא "כבויה" ואפשר "להדליקה" בעת הגדרת המכשיר הראשונית.

בעת התקנתן של אפליקציות שונות מערכת ההפעלה אנדרואיד דורשת מהמשתמש הרשאה לעשות שימוש בסוגי מידע שונים. המשתמש יכול להסכים להגדרות או לוותר על התקנת האפליקציה. אפליקציות של גורמים מפתחים שאינם חברת "גוגל" הן באחריות המפתחים, **כולל המידע שהאפליקציה אוספת על המשתמש, התראות הפרטיות ועוד.**

יצוין כי חברת "גוגל ישראל" השיבה על שאלות מרכז המחקר והמידע של הכנסת בפנייתו אליה לקראת הדיון. תשובת "גוגל ישראל" מציגה את השימוש בנתוני מיקום בהתאם לדברים שהוצגו בעדות בסנאט של ארצות-הברית והובאו לעיל בהרחבה.[14]

5. עמדת קבוצת העבודה של האיחוד האירופי בנושא הגנת מידע ופרטיות[15]

באיחוד האירופי פועלת קבוצת עבודה בנושא הגנת מידע ופרטיות. הקבוצה, שהוקמה מתוקפה של הדירקטיבה האירופית על הגנת מידע אישי (95/46/EC), היא גוף המייעץ לאיחוד האירופי בנושאי הגנת מידע ופרטיות. על מדינות האיחוד מוטלת האחריות לאמץ במסגרותיהן החוקיות את המלצות הקבוצה.

במאי 2011 פרסמה קבוצת העבודה נייר עמדה בנושא "שירותי מיקום במכשירי סלולר חכמים". להלן נקודות עיקריות במסמך זה:

[14] תשובת עו"ד דורון אבני, מנהל מדיניות וקשרי ממשל, "גוגל ישראל", מכתב, 20 בנובמבר 2011.

[15] **ARTICLE 29, Data Protection Working Party**, Opinion 13/2011 on "Geolocation services on smart mobile devices", Adopted on May 16, 2011.

- **נתוני מיקום במכשירי סלולר חכמים הם מידע אישי**. השילוב בין מידע על נקודות Wi-Fi ופרטי המידע הספציפיים של כרטיס רשת (כתובת MAC) הם מידע אישי ולכן נדרשת בעניין התייחסות מתאימה.
- **יש להבחין בין הגורמים המחזיקים בנתוני מיקום**: המחזיקים בתשתית נתוני מיקום (בפרט מיפוי נקודות Wi-Fi); מפתחי שירותים ואפליקציות המבוססות על מיקום; מפתחי מערכות הפעלה עבור מכשירי סמארטפון.
- **מידע על מיקום המצוי בטלפונים ניידים חכמים חושף פרטים אינטימיים על בעליהם ולכן נדרשת הסכמה מדעת**. הסכמה זו אינה יכולה להינתן כחלק מחתימה על תנאים כלליים. על ההסכמה להיות ספציפית ולתאום את עילת איסוף המידע. אם עילת איסוף המידע משתנה, נדרשת הסכמה חוזרת.
- **ברירת המחדל צריכה להיות שנתוני מיקום אינם נאספים.** מנגנונים שנדרשת בהם פעולה אקטיבית כדי למנוע את האיסוף (Opt-Out Mechanism) **אינם אמצעי הולם לקבלת הסכמה מדעת של המשתמש.**
- **קבלת הסכמתם מדעת של מועסקים ושל ילדים היא בעייתית.** על המעסיקים להשתמש בטכנולוגיות נתוני מיקום אם היישום שלהן הוא למטרה לגיטימית וניתנת להוכחה ואם אי-אפשר להשיג את המטרה באמצעים פולשניים פחות. אשר לילדים, על ההורים לבחון את הצידוק של שימוש באמצעים אלה ולכל הפחות ליידע את הילדים על כך. ככל הניתן, יש לאפשר לילדים להיות שותפים להחלטה על השימוש של ההורים בנתוני מיקום.
- **יש מקום להגביל בזמן את ההסכמה** ולהזכיר למשתמשים את הסכמתם לפחות אחת לשנה. נוסף על כך, יש ליידע את המשתמשים על מידת הדיוק של מידע המיקום.
- **יש לאפשר למשתמשים לוותר על הסכמתם לשימוש בנתוני מיקום** בקלות, בלא שיהיו לכך השלכות שליליות על השימוש שלהם במכשירי הקצה.
- **אשר למיפוי נקודות Wi-Fi, לחברות יש אינטרס לגיטימי לאסוף ולעבד כתובות MAC ונקודות Wi-Fi למטרת אספקת שירותים מבוססי מיקום, שכן זהו מידע הכרחי עבורן.** בשל איזון האינטרסים בין זכויות המחזיק במידע לזכויות המשתמש על המחזיק במידע לאפשר למשתמש שלא לחלוק עמו נתוני מיקום (Opt-Out) בקלות ולצמיתות, ללא דרישת מידע אישי נוסף ממנו.
- **על המידע על סוג הנתונים שנאספים – צורת האיסוף, משך האיסוף, מטרותיו ועוד – להיות ברור, מקיף וקל להבנה גם למשתמש הפשוט.**
- **לצדדים שלישיים, דוגמת דפדפנים ואתרי רשתות חברתיות, יש תפקיד מפתח בנוגע להצגתו ולאיכותו של המידע על שימוש בנתוני מיקום.**
- **המחזיקים בנתוני מיקום במכשירי סלולר צריכים לאפשר ללקוחותיהם גישה לנתוני המיקום שלהם בפורמט קריא ולהתיר להם את האפשרות לתקן או למחוק את המידע בלי לדרוש מידע אישי נוסף.**
- **למשתמשים יש זכות לגשת לפרופילים אפשריים המבוססים על נתוני המיקום שלהם, ולתקן או למחוק אותם. מומלץ לאפשר גישה מאובטחת למידע האמור באמצעות האינטרנט.**

- **על ספקי נתוני מיקום או שירותים המבוססים על מיקום להגדיר מדיניות שמירה על נתוני מיקום.** מדיניות זו תבטיח כי נתוני מיקום או פרופילים שנבנו על סמך נתוני מיקום יימחקו אחרי זמן הולם.
- **אם מפתחי מערכות ההפעלה או המחזיקים בתשתית נתוני מיקום מחזיקים בפרטים ספציפיים המאפשרים זיהוי חד-ערכי (כתובת MAC או כתובת זיהוי זמנית דוגמת UDID) הקשורים לנתוני המיקום האמורים, פרטי הזיהוי הייחודיים יישמרו לא יותר מ-24 שעות, למטרות תפעוליות.**

מרכז המחקר והמידע של הכנסת פנה למשרד התקשורת בשאלות לקראת הדיון. להלן עיקרי תשובת המשרד.

6. תשובת משרד התקשורת[16]

מרכז המחקר והמידע של הכנסת פנה למשרד התקשורת בשאלות לקראת הדיון. להלן עיקרי תשובת המשרד.

עוד לפני עידן הטלפונים החכמים היו בשוק שירותים המבוססים על מיקום, שהעניקו ללקוחותיהן חברות הסלולר. שירותים אלה היו מבוססים על מיקומו של הלקוח ביחס ל"אתר סלולרי", שממנו קיבל, באמצעות המכשיר, שירות סלולרי ברגע נתון.

ככל שמדובר בשירות הניתן על-ידי מפעיל רט"ן כלשהו (ללא קשר לאמצעים שבהם הוא ניתן), הרי שבתוקף הרשיונות הכלליים למתן שירותי רדיו טלפון נייד (רט"ן) ("הרשיונות הכלליים"), המפעילים מחויבים בקבלת אישור מהמשרד. נוסף על כך, **הרשיונות הכלליים מטילים חובות על מפעילי הרט"ן לשמור על פרטיות מנוייהם. זוהי חובה כללית, שאינה חלה רק במקרים של הענקת שירותים המבוססים על מיקום.**

כיוון שמכשירי סמארטפון אפשר להשתמש באפליקציות הניתנות על בסיס מיקומו של הלקוח גם ללא מעורבות או ידיעה של חברות הסלולר, הרי ששירותים רבים מסוג זה ניתנים על-ידי גורמים שונים שאינם חייבים ברשיון מכוח חוק התקשורת.

יש לעשות הבחנה בין שימוש בנתוני מיקום שנאספים בידי מפעילי הרט"ן במהלך אספקת שירותי תקשורת לכלל לקוחותיהם ובין יישומים המאפשרים מתן שירותים המבוססים על מיקום. אשר לסוג הראשון, הנושא מוסדר בדברי חקיקה שונים; **אשר לסוג השני, המשרד לא נתן את דעתו לנושא ספציפי זה.** עם זאת, **עמדת המשרד היא כי אין לעצור טכנולוגיות מתקדמות אשר יש בכוחן לקדם את ענף התקשורת, להגביר את רווחת הצרכן מהשימוש בשירותי תקשורת מתקדמים ולהעשיר את חוויית השימוש בשירותי התקשורת בישראל.**

מרכז המחקר והמידע של הכנסת פנה ל-3 חברות הסלולר הגדולות ("סלקום", "פלאפון" ו"פרטנר") בשאלות לקראת הדיון. להלן עיקרי תשובת החברות "פרטנר" ו"פלאפון".

[16] נתי ביאליסטוק כהן, יועץ בכיר למנכ"ל, משרד התקשורת, מכתב, 20 בנובמבר 2011.

7. תשובת חברת "פרטנר"[17]

חברת "פרטנר" אינה שותפה, ואינה יכולה להיות שותפה, להגדרת ברירות המחדל ואפשרויות השימוש לגבי נתוני מיקום במכשירי הסמארטפון של משתמשיה; הדבר מצוי בשליטתם הבלעדית של יצרני המכשירים.

"פרטנר", כמפתחת אפליקציות וכרוכשת אפליקציות ממפתחים אחרים, מקפידה על שמירת הפרטיות של לקוחותיה. **הגישה לנתוני מיקום במסגרת השימוש באפליקציות המבוססות על מיקום תלויה בהסכמתו המפורשת של המנוי, באופן מוחלט, וביכולתו להפסיק את השימוש באפליקציה ואת הדיווח והאיכון בכל זמן נתון ולפי שיקול דעתו האישי בלבד.**

אשר להעברת מידע לצדדים שלישיים ציינה "פרטנר" כי היא מעבירה מידע כאמור בכפוף לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007, או בהתאם לצווים שיפוטיים בנושא.

"פרטנר" אינה מוסרת נתוני מיקום לגורמים אחרים (שלא במסגרת החוק דלעיל) אלא אם כן הנתונים נמסרים באופן שאינו מאפשר את זיהוי המנוי ואין בו נתונים אישיים כמו מס' טלפון נייד או שם המנוי או שהדבר הנעשה בהסכמתו של המנוי.

8. תשובת חברת "פלאפון"[18]

בעיקרון "פלאפון" אינה שותפה להגדרת ברירות המחדל ואפשרויות השימוש במכשירי הקצה של משתמשיה. "פלאפון" מעדכנת באמצעות המכשיר הנרכש דרכה את פרטי השרתים שלה, כדי שאם הלקוח יחפוץ בעתיד להצטרף לשירותים שנעשה בהם שימוש במיקום, שליחת המיקום על-ידי המכשיר לצורך קבלת השירות תיעשה לשרת המתאים ב"פלאפון". אם הלקוח אינו מצטרף לשירותים אלו, הגדרת השרת נשארת "פסיבית" ולא באה לידי מימוש. **"פלאפון" איננה מגדירה את אפשרויות שמירת נתוני המיקום על גבי מכשיריה.**

נתוני האיכון ברשת הסלולר "נדרסים", כלומר הנתון המעודכן ביותר מוחק את קודמו. בשירותים המבוססים על מיקום תיתכן שמירה של המידע, כנגזרת של סוג השירות וצרכיו (למשל – העברת דוחות נוכחות חודשיים בשירות "שעון נוכחות נייד"). המידע נשמר במערכות מאובטחות, והגישה אליהן מוגבלת ואפשרית בהרשאות פרטניות בלבד.

יש לזכור כי טכנולוגיית הסלולר מבוססת על איכון המכשיר לשם אספקת שירותי הסלולר (שיחות, הודעות וכו'). למשתמש אין שליטה על ביטול מידע זה. כאמור, **ברירת המחדל היא שהמיקום מדווח לרשת, שכן ללא דיווח לא קיים שירות סלולרי. והמידע המעודכן "דורס" את קודמו.** אשר לשירותים המבוססים על מיקום (כגון שעון נוכחות נייד, ניווט וכו'), המידע נשמר בהתאם להגדרות השירות אך ורק לגבי מנויים המשתמשים בשירות הספציפי. ללקוח אין גישה לנטרול המידע הנשמר במסגרת השירות.

"פלאפון" איננה חולקת מידע כאמור עם צדדים שלישיים. אם הלקוח מצטרף במודע לשירות המבוסס על מיקום ומסופק על-ידי ספק שירות שאיננו "פלאפון", המיקום נמסר לספק השירות, אך זאת אך ורק במסגרת הפעלת השירות על-ידי הלקוח ובמהלכו.

---

[17] עו"ד יהל בן-נר, מנהלת אגף רגולציה וקשרי מפעילים, "פרטנר תקשורת", מכתב, 20 בנובמבר 2011.

[18] יוליה מרוז, מנהלת אגף רגולציה, "פלאפון", דוא"ל, 20 בנובמבר 2011. המידע מחברת "פלאפון" נתקבל לאחר השלמת המסמך ועודכן רק לאחר הדיון.

9. תשובת "מיקרוסופט"[19]

לדברי נציגת חברת "מיקרוסופט ישראל", מערכת ההפעלה החדשה לסלולר (Windows Phone 7), טרם הושקה בישראל. בשל כך, ובשל לוח הזמנים הקצר, אין באפשרות החברה להשיב תשובה מפורטת על שאלות מרכז המחקר והמידע של הכנסת.

סיכום

בעבר נדמה היה כי האינטרנט מאפשרת פרטיות חסרת תקדים. ביטוי אנונימי בסוגיות שונות, רכישות ותשלום חשבונות, זהות מקוונת פיקטיבית, חיפוש מידע בנושאים רבים ועוד – את כולם יכול האדם לקיים מחדרו הפרטי, ללא צורך בחשיפה ישירה. ואולם, הפרטיות באינטרנט היא בעיקרה אשליה: מנגנוני איסוף מידע רבים פועלים ברשת זה כבר ומנגנונים מתקדמים יותר מפותחים כל העת. אלה מתעדים את האתרים שבהם אנו גולשים, את העסקאות שאנו מבצעים, ואת תחומי העניין ודפוסי התקשורת שלנו.

למרות אשליית הפרטיות אנו מותירים אחרינו "טביעת רגל" דיגיטלית (Digital Footprint) בגלישתנו באינטרנט.

הקלות היחסית שבאיסוף מידע על אדם או גורם כלשהו ומסות המידע הנצברות הופכות גם פריטי מידע טריוויאליים לבעלי משמעות ולכאלה המאיימים על הפרטיות. **נתוני מיקום הם אחד מפריטי המידע האישיים ביותר. כאמור לעיל, שילובם של נתוני מיקום עם מידע נוסף יכול להוביל לחדירה מועצמת לפרטיותו של האדם.**

עם זאת, **מושג הפרטיות עצמו מצוי כיום במשא-ומתן חברתי, תרבותי ומסחרי ער. לא רק גופים מסחריים בעלי עניין אלא גם חלק לא מבוטל ממשתמשי הקצה רואים בתפיסת הפרטיות הרווחת תפיסה אנכרוניסטית.** גורמים אלה מדגישים את היתרונות שבוויתור על הפרטיות עבור משתמש הקצה כפרט ועבור השוק כמכלול.

על המחוקק והרגולטור מוטלת האחריות למצוא את מערך האיזונים בין צורכי המשתמש הפרטי ובין צורכי השוק. על פני הדברים, יש סתירה מובנית בין הרצון של גורמי השוק "לדעת הכול" על המשתמשים שלהם ובין רצון המשתמש "להסתיר ככל יכולתו". בפועל, התמונה מורכבת יותר, כיוון שקיימים משתמשים מסוגים שונים: מחד גיסא, יש מי שאינם ערים לפגיעה בפרטיותם, ומאידך גיסא, יש המוכנים לוותר עליה בשל התועלת המרובה שהם מפיקים מנתוני מיקום.

בלי לנקוט עמדה בסוגיות מורכבות אלה, נראה כי אפשר להגדיר כמה עקרונות מנחים להתמודדות עם הסוגיה, ואלה עולים מן האמור במסמך:

שקיפות: למשתמש הקצה יש מלוא הזכות לקבל מידע מלא, קריא ובהיר על המידע הנאסף עליו, בפרט בנוגע לנתוני מיקום.

---

[19] אורלי פרידמן מרטון, יועצת משפטית ומהלת קשרי ממשל, "מיקרוסופט ישראל", דוא"ל, 20 בנובמבר 2011.

בחירה: יש לאפשר למשתמש הקצה לבחור בין האפשרות שיהיה איסוף של נתוני המיקום שלו לבין האפשרות שנתונים אלו לא ייאספו. בחירה אמיתית אין משמעה "הכול או לא כלום" אלא יש ליצור מרחב של אפשרויות.

הגבלות על היקף המידע הנאסף: יש לבחון הטלה של מגבלות על סוג המידע הנאסף, על מידת הפירוט שלו, היקפו ועל ההצדקה שבאיסופו, וכמו כן יש לוודא את האנונימיות של מידע זה.