ספטמבר 2022

לכבוד

הרשות להגנת הצרכן ולסחר הוגן

לידי: עו"ד מיכאל אטלן - הממונה על הרשות להגנת הצרכן ולסחר הוגן

נייר עמדה בנושא:

חובות גילוי בעניין סיכונים של האינטרנט של הדברים (IoT)

מרכז רנה ומאיר חת לחקר התחרות והרגולציה, המסלול האקדמי – המכללה למינהל
טלפון: 03-9634104 | דוא"ל המרכז: hethcenter@colman.ac.il
רח' אלי ויזל 2, ראשון לציון | בקרו אותנו באתר: www.colman.ac.il/heth_center
עמוד הפייסבוק: https://www.facebook.com/hethcenter/

מרכז חת
לחקר התחרות והרגולציה
המסלול האקדמי המכללה למינהל

מרכז חת הינו מוקד אקדמי רב תחומי של המסלול האקדמי המכללה למינהל. המרכז נוסד ביוזמתם והודות לתרומתם של גב' רנה ופרופ' מאיר חת.
תכליתו של מרכז חת היא פיתוח והעברת ידע בתחומי התחרות והרגולציה, על היבטיהם התיאורטיים והמעשיים.
המרכז הוקם מתוך רצון לחקור ולהעמיק את ההבנה על אודות התחלופה וההפעלה של אמצעי התחרות והרגולציה בשווקים שונים בישראל.
המטרה היא לחדד בעיות הטעונות פתרון, ולגבש המלצות לשיפור המדיניות הרגולטורית הראויה.

השופטת בדימוס ד"ר איריס סורוקר

מרכז רנה ומאיר חת לחקר התחרות והרגולציה

facebook.com/hethcenter 03-9634104

colman.ac.il/heth_center hethcenter@colman.ac.il

ספטמבר 2022

לכבוד

עו"ד מיכאל אטלן

הממונה על הרשות להגנת הצרכן ולסחר הוגן

כללי

בנייר עמדה זה נבקש להתייחס לטיוטת הנחיה שפורסמה להערות הציבור ביום 24.7.22 על ידי הרשות להגנת הצרכן ולסחר הוגן בעניין חובת הגילוי לגבי סיכוני מוצרי IoT - "האינטרנט של הדברים".

להלן נסקור את הסיכונים המרכזיים המוכרים של האינטרנט של הדברים (IoT), נסכם את העמדות העיקריות למיתון הסיכונים בישראל, באירופה ובארה"ב ונסיים עם המלצותינו.

האינטרנט של הדברים (IoT)

"האינטרנט של הדברים", מונח שהוטבע על ידי קווין אשטון בשנת 1999,[1] הוא כינוי ידוע לטכנולוגיה מתקדמת המאפשרת לחפצים, מוצרים והתקנים שונים ("דברים") להתחבר אל האינטרנט. החיבור מאפשר לחפץ מוחשי לקלוט ולאסוף מידע מהסביבה הפיסית (באמצעות חיישנים), ולהעביר את המידע לרשת לצורך עיבוד, הסקת מסקנות, ניתוח נתונים ושימוש בהם (באמצעות תוכנות).[2] האינטרנט של הדברים מאפשר ליצור תקשורת דו-כיוונית בין חפץ לחפצים אחרים, בין חפץ לאתרים ברשת, ובין חפץ למשתמשים שונים. לכך דוגמאות רבות.[3] למשל: צמיד דיגיטלי המוצמד לכף-יד עשוי לנטר נתונים גופניים כמו טמפרטורה, דופק ולחץ דם, ולשדר את המידע לרשת לצורך עיבוד והסקת מסקנות רפואיות

[1] That 'Internet of Things' Thing - RFID JOURNAL

[2] הרשות הפדרלית למסחר בארצות הברית, ה- FTC, הגדירה כך את האינטרנט של הדברים, בדו"ח מינואר 2015:
"The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day."

[3] לסקירת תחומי תוכן ופיתוחים של האינטרנט של הדברים, ראו למשל:

Visions and Challenges for Realizing the Internet of the Things (2010), editors: Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelffle; sec. 3.2

מרכז רנה ומאיר חת לחקר התחרות והרגולציה, המסלול האקדמי – המכללה למינהל
טלפון: 03-9634104 | דוא"ל המרכז: hethcenter@colman.ac.il
רח' אלי ויזל 2, ראשון לציון | בקרו אותנו באתר: www.colman.ac.il/heth_center
עמוד הפייסבוק: https://www.facebook.com/hethcenter/

כמו גם להעבירו דרך האינטרנט לגורמים רלבנטיים (כמו עונד השעון או הרופא); טלפון חכם מסוגל לספור ולסכום את צעדי ההליכה של המשתמש האוחז בו, לדווח להולך על הישגיו היומיים ולהמליץ המלצות בתחום הבריאות והספורט, ועוד.

בעשור האחרון חלה התפתחות טכנולוגית משמעותית שהביאה לגידול במספר המכשירים המחוברים לאינטרנט; ובשנים האחרונות חלה התפתחות מהירה נוספת שהביאה ליכולות טכנולוגיות הכוללות אלגוריתמים מתקדמים של בינה מלאכותית, למידה עמוקה ופריסת רשתות 5G שמאפשרות למכשירים להעביר ולנתח נתונים בקצב מהיר.[4]

ה"אינטרנט של הדברים" הולך וחודר אל עולמות תוכן רבים ומגוונים, ודומה כי האפשרויות הולכות ונפתחות: תחום הבריאות (כגון ניטור נתונים גופניים וטיפול במחלות); תחום הבטיחות (למשל איתור דליפות של חומרים מסוכנים או קרינה); תחום המסחר (כמו ניהול מלאי וקידום מכירות); תחום תשתיות האנרגיה (מעקב וניהול מערכות כמו חשמל, קירור, גז); תחום החקלאות (למשל ניטור ודיווח על דליפות מים מצינורות השקיה וכן איתור מזיקים); תחום איכות הסביבה (ניטור וניתוח נתוני זיהום והפצת אזהרות); תחום הצריכה הקמעונאית (עגלת קניות וירטואלית); תחום התחבורה (רכבים אוטונומיים, תחבורה מותאמת אישית, צמתי תנועה חכמים); תחום הדיור (כגון הבית החכם); התחום העירוני (העיר החכמה), ועוד.

הצפי הוא כי 75 ביליון מכשירים יהיו מחוברים ל-IoT בשנת 2026[5], ותחזיות כלכליות מעריכות שתעשייה זו תגיע למאות מיליארדי דולרים בעשורים הקרובים.[6]

סיכונים בשימוש של מוצרי ושירותי IoT

לצד התועלות הרבות הקיימות לאינטרנט של הדברים, הוא מייצר סיכונים לא מבוטלים. שני הסיכונים המרכזיים[7] [8] [9] לצרכן והרלוונטיים ביותר בקשר עם הצורך בחובות גילוי הם:

Daniele Miorandi, Sabrina Sicari, Francesco de Pallegrini, Imrich Clamtac, "The Internet of Things: Visions, Applications and Research Challenges" (2012)

יניב אביטל, "10 דוגמאות מוצלחות לאינטרנט של הדברים" (2014).

[4] ערך "האינטרנט של הדברים" בויקיפדיה

[5] statistica research

[6] ראו למשל סקירה של תחזיות כלכליות של חב' המחקר גרטנר, חב' הייעוץ מקינזי וכן של חב' סיסקו המופיעות בוויקיפדיה, בערך "האינטרנט של הדברים".

[7] ראו:

" We Asked Executives About The Internet of Things And Their Answers Reveal That Security Remains A Huge Concern" *Business Insider*. Retrieved 26 June 2015.

א. סיכונים הקשורים לאבטחת מידע - החשש לפריצה למערכות האינטרנט, לפגיעה בתפקודי המערכת, לגניבת מידע ולשימוש בלתי מורשה במידע. לא רק שחפצים המחוברים לאינטרנט יכולים לשמש למתקפות היכולות לאפשר שימוש לרעה במידע, אלא שהחדירה באמצעות חיבורים לIoT יכולה לאפשר התקפה על מתקני תשתיות ומתקנים מרכזיים.

ב. פגיעה בפרטיות והגנת הצרכן[10] - האינטרנט של הדברים מאפשר לנטר ולאסוף מידע שוטף על המשתמש (כמו נתוני בריאות, צריכה, הרגלים, מיקום). המידע עשוי להיות בעל אופי אישי ופרטי. דליפת מידע, העברת מידע לצדדים שלישיים, שימוש משני או שימוש מסחרי במידע וכל שימוש שאינו שקוף או בלתי מורשה, עלולים לפגוע ברווחת הפרט.

סיכון נוסף אותו יש לציין הוא **פגיעה בבטיחות הצרכן**[11] - מערכות ה-IoT כוללות בין היתר אפליקציות חכמות אשר מתקשרות עם חיישנים ועלולות להיות תקולות, ליצור אינטראקציות שגויות עם מכשירים או לגרום לכשלים אחרים בתקשורת מערכת ה-IoT. כשלים טכניים עלולים ליצור סכנת בטיחות פיזית לצרכן.

בנוסף קיימים סיכונים נוספים לחברה ולסביבה, כגון: **איום על התהליך התחרותי במשק -** אפקט הרשת, לצד איסוף אינטנסיבי של מידע בידי גופים מסחריים, הם כר פורה להיווצרות גופים מונופוליסטיים חזקים; **סיכונים הקשורים לאתיקה -** קבלת החלטות אוטומטיות המבוצעת בהתאם לאלגוריתם שתוכנת על ידי יוצר החפץ; **סיכונים הקשורים לקיימות -** עצם ייצורם של מוצרים אשר הם חלק מה-IoT אשר מערבים תהליכים טכנולוגיים הדורשים שימוש במתכות כבדות וכימיקלים שאינם ניתנים למיחזור.[12]

---

[8] ראו:
V. Lara. What the internet of things means for consumer privacy. https: //perspectives.eiu.com/technology - innovation/what - internet - things - means-consumer-privacy-0/white-paper/what-internet-things-meansconsumer-privacy, March 2018.

[9] ראו:
Feamster, Nick (18 February 2017), Freedom to Tinker "Mitigating the Increasing Risks of an Insecure Internet of Things"

[10] ראו:
J. Caltrider .10 fascinating things we learned when we asked the world "how connected are you?" November 2017

[11] ראו:
Nguyen, D. T., Song, C., Qian, Z., Krishnamurthy, S. V., Colbert, E. J., & McDaniel, P. (2018, December). IotSan: Fortifying the safety of IoT systems. In Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (pp. 191-203).

[12] ראו:
ght, A.; Rowland, C. (2015). "Chapter 11: Responsible IoT Design". In Rowland, C.; Goodman, E.; Charlier, M.; et al. (eds.). Designing Connected Products: UX for the Consumer Internet of Things. O'Reilly Media. pp. 457–64. ISBN 9781449372569.

<u>חובות גילוי לגבי סיכוני IoT בעולם</u>

התגברות תקיפות הסייבר (עליה של 300% רק בשנת 2019[13]), דחפה להתקדמות עולמית בנושא רגולציה של IoT.

<u>בארה"ב</u>:

בינואר 2015 פורסמו המלצות של ה- FTC בנוגע ל- IoT ואשר מיועדות לחברות היצרניות:[14]

- בעת תהליכי הייצור יש לוודא את אבטחת איסוף, אחסון ועיבוד הנתונים. יש לוודא הצפנת מידע בכל שלב ("Defense in Depth Approach");

- חברות IoT רשאיות לאסוף רק נתונים שהן חייבות ולהגביל את הזמן שבו הן מחזיקות את הנתונים.

- **יש לאפשר למשתמשים לבחור אילו נתונים הם מסכימים כי ישותפו עם IoT והם צריכים להיות מיודעים אם הנתונים שלהם נחשפים.** זו ההמלצה הרלוונטית ביותר מבחינת חובת הגילוי.

יושם אל לב כי מדובר בהמלצות ולא בהוראות מחייבות.

בשנת 2020 אושר החוק הפדרלי Internet of Things (IoT) Cybersecurity Improvement Act of 2020 אשר קובע מסגרת חקיקתית כללית לסטנדרטים שידרשו לגבי שימוש וניהול מערכות IoT בממשל הפדרלי וסוכנויותיו (ללא התייחסות מיוחדת לחובת גילוי). החוק מורה לשני גופים, ה-NIST (National Institute for Standards and Technology) וה-OMB (Office of Management and Budget) לפתח ולפרסם הנחיות מתאימות ולפקח על יישומן. אכיפת החוק תחל מדצמבר 2022; זהו החוק הפדרלי הראשון בנושא ועל אף שהוא מתייחס בעיקר למגזר הציבורי, צפוי שישפיע גם על המגזר הפרטי, היות והסטנדרטים הפדרליים מנחים את הסטנדרטים הנהוגים בתעשייה לאור השאיפה לאחידות ויעילות מירבית.

עוד לפני חקיקת חוק זה, שתי מדינות בארה"ב (קליפורניה ואורגון) חוקקו חוקים המתייחסים לחובת יצרני IoT לעשות שימוש באמצעי אבטחת מידע סבירים בקשר למידע שנאסף או לגילויו. הצעות לחוקים מדינתיים נוספים או תיקונים לחוקים מדינתיים קיימים, העוסקים בהגנת הצרכן במוצרי IoT (אך לאו

---

[13] ראו:

https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

[14] ראו:

FTC Staff report, "Internet of Things – Privacy & Security in connected World", January 2015

דווקא עוסקים ישירות בחובת הגילוי) תלויים ועומדים באילינוי, ניו יורק ואוהיו. בקליפורניה ובפנסילבניה תלויות ועומדות הצעות חוק מדינתיות העוסקות במוצרי IoT, לרבות התייחסות מפורשת לחובת הגילוי לצרכן.[15]

צו נשיאותי ממאי 2021, שמטרתו שיפור אבטחת המידע ברמה הלאומית (Improving the Nation's Cybersecurity (14028),[16] דורש מגופים וסוכנויות ממשלתיים לקדם את אבטחת המידע באמצעות יזום תוכניות שונות. מכון ה- NIST התבקש לפרסם הנחיות לקידום פרקטיקות אבטחת מידע ובנוסף ליזום תוכניות המיועדות ליידוע צרכנים על אבטחת המוצרים בהקשר של IoT. בהתאם לכך פרסם NIST בפברואר 2022 טיוטה בנוגע להדבקת תוויות על מוצרי IoT[17] ובמאי 2022 פירסם המכון את סיכום ההמלצות.[18] מטרת התוויות היא לאפשר לצרכנים לקבל מידע רלבנטי לקבלת החלטות קניה של מוצרי IoT ובכך לעודד שקיפות ואת אמון הצרכנים במוצרי IoT, לצד ניהול סיכונים של אבטחת המידע. המלצות ליצרנים להדבקת תוויות כוללות מידע הקשור לחלקו של הצרכן באחריות לשימוש במוצר והוראות לצרכן הקשורות לגבי סיום חיי המוצר.[19] בהמשך ובהתאמה להנחיות ה-NIST, תלויה ועומדת הצעת חוק מדינתית בקליפורניה המתייחסת לאבטחת מידע של IoT. בתוך כך, החוק מכיל הוראות בדבר הצמדת תוויות מידע על מוצרים.[20]

מסמכים נוספים ותוצרי סדנאות של NIST מעידים על תהליך עבודה נמשך בנושא שיפור אבטחת המידע של מוצרי IoT שטרם הסתיים.[21]

יצוין כי במספר מדינות בארה"ב קיימים חוקים המעגנים את פרטיות הצרכן: בקליפורניה קיים חוק משנת 2018: California Consumer Privacy Act[22] המעגן את זכויות תושבי קליפורניה לקבל מידע על

---

[15] ראו:

https://custom.statenet.com/public/resources.cgi?id=ID:bill:PA2021000H1908&ciq=ncsl&client_md=0268744c063ccce568c7a65549702956&mode=current_text

[16] ראו:

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[17] ראו:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

[18] ראו:

https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity

[19] ראו:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf
עמודים 18-20

[20] ראו:

https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx

[21] ראו:

https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/timeline

איסוף מידע אישי, סירוב למכירת המידע, גישה למידע אישי שלהם ודרישה מעסק למחוק מידע אישי. חוקים דומים נחקקו בקולורדו, קונטיקט, וירג׳יניה ויוטה והם צפויים להיכנס לתוקף בשנת 2023. [23]

באירופה[24]:

חוק ה- General Data Protection Regulation (GDPR) משנת 2016[25] קובע הוראות מחייבות במטרה להגן על תושבי האיחוד האירופי בנוגע לעיבוד נתונים אישיים שלהם.[26] החוק מתייחס לאיסוף, שמירה והעברה של נתונים אישיים של אנשים פרטיים המתגוררים באיחוד האירופי וקובע כללים להגנה על פרטיות המידע האישי. שני עקרונות העומדים בבסיס ה-GDPR הם פרטיות ואבטחת מידע ומתוכם נגזרים שורת כללים מחייבים, כגון: חובה לקבל הסכמה של המשתמש לאיסוף מידע; איסוף מינימום מידע; שקיפות בתהליך עיבוד המידע והזכות להישכח. על אף שה-GDPR מחייב להודיע לאנשים על שמירת נתוניהם או העברתם לצדדים שלישיים, נראה כי ה-GDPR אינו מספק הגנה מלאה למשתמשים במוצרי IoT. אחת הסיבות לכך היא שה-GDPR מיועד בעיקר להגנת הפרטיות ואין בו התייחסות לכל סיכוני אבטחת המידע הנובעים באופן ספציפי מהשימוש ב-IoT[27] יצוין כי בשלב זה חסרים נתונים על היקף הציות של יצרני ה-IoT לרגולציה מכח ה-GDPR ונדרש מחקר אמפירי שיבחן את האפקטיביות של רגולציה זו לטובת ההגנה על הצרכנים.[28]

בנובמבר 2020 פרסם ארגון ה-ENISA (European Union Agency for Network and Information Security) הנחיות לאבטחת מידע במוצרי IoT.[29] ההנחה ביסודן היא שלחלק ניכר מהצרכנים אין מודעות או ידע לגבי ההשלכות של אבטחת מידע. לכן, נקבע שאין להטיל את האחריות לכשלי אבטחה על המשתמשים אלא שעל ארגונים להשקיע משאבים כדי לעורר את מודעות הצרכנים לחשיבות אבטחת

---

[22] בשנת 2020 עבר תיקון לחוק אשר אף מגדיל את שליטת תושבי קליפורניה במידע האישי שלהם.

[23] ראו:

https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx

[24] האיחוד האירופי נוקט במודל רגולטורי שונה ממדינות אחרות ולעניין זה ראו:

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092-1110.

[25] אכיפת החוק החלה בשנת 2018

[26] ערך GDPR בויקיפדיה

[27] ראו:

Bastos, D., Giubilo, F., Shackleton, M., & El-Moussa, F. (2018, December). GDPR privacy implications for the Internet of Things. In *4th Annual IoT Security Foundation Conference* (Vol. 4, pp. 1-8).

[28] ראו:

Gupta, S., & Ghanavati, S. (2022). Privacy in the Internet of Things: Where do We Stand? A Systematic Literature Review.

[29] ראו:

https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

מידע נאותה, באמצעים שיווקים ובאמצעות הדרכה למשתמשים. בנוסף הוצע כי יצרנים יוסיפו למוצרים מדריך ברור אשר מסביר את השימוש במוצרים ובדרך זו יקודם עקרון השקיפות כלפי הצרכנים.

<u>בבריטניה:</u> בשנת 2018 פירסם המשרד הממשלתי הבריטי ל-Digital, Culture, Media & Sport הנחיות לפרקטיקות בהן יש לנקוט כלפי צרכנים לגבי מוצרי ושירותי IoT.[30] במסגרת 13 הנחיות שפורסמו, הוזכרו חובות גילוי שונות כלפי הצרכנים ובהן: תיאור חולשות המוצר, תמיכה בעדכונים של המוצר, ומתן הוראות ברורות כיצד מוחקים מידע אישי. בנובמבר 2021 הוצעה בבריטניה הצעת החוק (שעדיין לא אושרה) אשר מסדירה אבטחת מידע של IoT: product Security and Telecommunications Infrastructure ("PSTI") Bill.[31]

<u>ספרות מחקרית רלוונטית</u>

קיימת ספרות מחקרית מתפתחת אשר סוקרת ודנה בסיכונים הנובעים מ-IoT ואף מציעה פתרונות. חלק מהספרות עוסקת בהעלאת פתרונות טכניים[32]; וחלקה עוסקת ברגולציה אגב ניתוח הסיכונים לצרכן[33] ובוחנת את הסוגיה של הטלת חובות גילוי כחלק מהאינפורמציה הנדרשת לצרכן לקבלת החלטות הצריכה.

אחת האפשרויות הרגולטוריות היא להטיל חובה להצמיד תוויות מידע על מוצרי IoT. במחקר שפורסם בשנת 2020[34] המתבסס על ראיונות עם מומחים לפרטיות ולאבטחת מידע וכן עם צרכנים, חוקרים יצרו תבניות של תוויות מידע: תווית אחת כוללת מידע ראשוני החשוב ביותר והיא מיועדת להצגה על המוצר עצמו או באופן בולט באתר המוצר. תווית שניה כוללת מידע שניוני שיוצג באופן מקוון באמצעות קישור או קוד לסריקה. המידע הראשוני כולל: פרטים אודות התקופה בה יסופקו עדכונים למכשיר, סוג המידע

---

[30] ראו:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[31] Product Security and Telecommunications Infrastructure (PSTI) Bill

[32] ראו:
Gupta, S., & Ghanavati, S. (2022). Privacy in the Internet of Things: Where do We Stand? A Systematic Literature Review.

[33] ראו:
Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?. *Big Data & Society*, *9*(1), 20539517221108369.

[34] ראו:
Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020, May). Ask the experts: What should be on an IoT privacy and security label?. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 447-464). IEEE.

שיאסף, מטרת איסוף המידע, רמת הפירוט של המידע הנאסף, היכן ישמר המידע ועוד. המידע השניוני כולל למשל את תדירות איסוף המידע והתאמת המכשיר לסטנדרטים וחוקים (כגון GDPR).

בנספח א׳ להלן מופיעים שני סוגי התוויות שהוצעו במאמר.[35]

מחקר נוסף שבדק את השפעת הגילוי באמצעות תוויות המידע על נכונות הצרכנים לקנות מוצרי IoT, מצא כי הצרכנים יעדיפו לרכוש מוצרים שמוצמדת אליהם תווית מידע יותר מאשר מוצרים שלא מוצמדת אליהם תווית מידע. חלק מהתוויות מעודדות מוכנות לשלם יותר, לעומת מוצרים אחרים.[36]

מחקר חדש שפורסם ב-2022 מציג סיכוני IoT ספציפיים לעיתונאים:[37] חשיפת מידע חסוי שנמצא בידי עיתונאים לרבות חשיפת מקורות עיתונאים חסויים. כותבי המאמר מציינים שקיימת סכנה אמיתית ליציבות החברתית ולעקרונות הדמוקרטיה אם יפגע החופש העיתונאי. למרות זאת, עיתונאים אינם מודעים לסיכוני ה- IoT ומכאן שגם אינם פועלים כדי להסירם או לצמצמם.

המאמר מעלה את השאלה אם יש צורך בהתייחסות ספציפית במסגרת ההנחיות לחובת גילוי גם לקבוצות מסוימות (לרבות מקצועות או קבוצות מסוג אחר) החשופות לסיכונים מיוחדים.

נקודה זו מקבלת חיזוק נוסף במאמר אוסטרלי[38] משנת 2022 אשר מזהה קבוצות רגישות לסיכוני IoT: קשישים וילדים וכן אנשים (בד״כ נשים) הסובלים מאלימות במשפחה, אשר מוצרי IoT יכולים להגביר הטרדות ומעקב אחריהם.

<u>חובות גילוי בישראל</u>

חוק הגנת הצרכן, התשמ״א-1981 נועד להגן על ציבור הצרכנים מפני הטעיה וניצול על ידי העוסקים; להסדיר יחסי צרכנות הוגנים; ולמתן כשלי שוק בעסקאות המבוססות על אי-סימטריה במידע. ביסוד החוק ניצבת מצוקת הצרכנים, המצויים בנחיתות יחסית מבחינת כושר המיקוח והמידע שברשותם, לעומת כוחם של העוסקים, המרכזים בידיהם מידע רלבנטי להתקשרות. החובות שמטיל החוק חלות בעיקר על עוסק – שמוגדר: ״מי שמוכר נכס או נותן שירות דרך עיסוק, כולל יצרן״. (סעיף 1 לחוק)[39].

---

[35] ניתן לראות את התוויות גם באתר: https://www.iotsecurityprivacy.org

[36] ראו:

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PloS one*, *15*(1), e0227800.

[37] ראו:

Shere, A. R., Nurse, J. R., & Martin, A. (2022). Threats to Journalists from the Consumer Internet of Things.

[38] ראו:

Harkin, D., Mann, M., & Warren, I. (2022). Consumer IoT and its under-regulation: Findings from an Australian study. *Policy & Internet*, *14*(1), 96-113.

[39] ערך "חוק הגנת הצרכן" בויקיפדיה

סעיף 4 לחוק קובע את היקף חובת הגילוי שחלה על העוסק כלפי הצרכן. העוסק חייב בחובת גילוי של כל *פרט מהותי* בעיסקה, ובעיסקה מתמשכת חלות הוראות מיוחדות (סעיף 13ג לחוק). החובות המוטלות על העוסק עולות בקנה אחד עם דיני החוזים הכלליים הנהוגים בישראל, אשר ככלל מחייבים את הצד המיודע לגלות לצד שכנגד פרטים מהותיים הקשורים לעיסקה ולתמחורה, ואשר עשויים להשפיע על החלטת ההתקשרות (סעיפים 14, 15 ו- 39 לחוק החוזים (חלק כללי), התשל"ג- 1973).

סעיף 4(א)(2) לחוק הגנת הצרכן קובע כי "עוסק חייב לגלות לצרכן "כל תכונה בנכס החייבת החזקה או שימוש בדרך מיוחדת כדי למנוע פגיעה למשתמש בו או לאדם אחר או לנכס תוך שימוש רגיל או טיפול רגיל". **טיוטת ההנחיה שהוציא הממונה משתלבת בהוראת חוק זו**, שעה שההנחיה קובעת: "לנוכח הסיכונים הממשיים שעלולים להיגרם בשל תקיפות סייבר נגד מוצרי IoT ניתן לומר כי מדובר בתכונה במוצר המחייבת החזקה או שימוש בדרך מיוחדת. ההחזקה והשימוש כאמור נדרשים כדי למנוע פגיעה בצרכן או במוצר עצמו...".

ואמנם, שווקים דיגיטליים (השווקים בהם נסחרים מוצרי ה-IoT), סובלים מבעיה של חוסר מידע הנדרש לצרכנים לצורך ביצוע עסקאות מושכלות. חובות הגילוי הרלבנטיות להתגברות על חסר זה הן משני סוגים[40]: חובת גילוי כללית של פרטים מהותיים שאי גילויים עלול להטעות את הצרכנים (זאת מכוח סעיף 2(א) לחוק); וחובת גילוי של רשימה מפורטת של סוגי מידע החייבים בגילוי (מכוח סעיף 4): (1) כל פגם או איכות נחותה או תכונה אחרת הידועים לו, המפחיתים באופן משמעותי מערכו של הנכס; (2) כל תכונה בנכס המחייבת החזקה או שימוש בדרך מיוחדת כדי למנוע פגיעה למשתמש בו או לאדם אחר או לנכס תוך שימוש רגיל או טיפול רגיל; (3) כל פרט מהותי לגבי נכס שקבע השר באישור ועדת הכלכלה של הכנסת.

ברשימה (חלקית) להלן, נפרט סוגי מידע מהותי לעסקאות צרכניות בשווקים הדיגיטליים (בפרט IoT) ואשר דרושים לצרכן ממוצע לצורך קבלת החלטות, אך אינם נכללים במפורש בחובות הגילוי המפורטות בסעיף 4 לחוק הגנת הצרכן:

(א) מידע הנוגע לסיכונים מערכתיים (תקלות מערכתיות) הכרוכים בביצוע העסקאות הצרכניות בשווקים הדיגיטליים - מידע זה כולל את קיומם של הסיכונים, ההסתברות להתרחשותם, והאמצעים הננקטים לצורך מניעת התרחשותם.

(ב) מידע אודות זהות הצדדים לעיסקה - מי היא הפירמה המוכרת את המוצר או השירות? למרות שסעיף 2(א)(6) לחוק הגנת הצרכן מטיל על העוסק את החובה לגלות את זהות היצרן, היבואן או נותן השירות, עלולה להיווצר בעיה של זהות המוכר, לדוגמא, במקרים שבהם המוכרים הם קניונים וירטואליים. במקרים אלו לכאורה לא מוטלת עליהם חובת זיהוי שכן הם אינם המוכרים אלא גורם אחר.

[40] אמל ג'אברין, דיני המסחר האלקטרוני הצרכני (2015), פרק חמישי, עמ' 649

(ג) מידע אינפורמטיבי על אודות הפירמה ודרכי ההתקשרות עימה - בשווקים דיגיטליים התקשורת מתבצעת לרוב באמצעים דיגיטליים ולכן יש לחייב את העוסק לגלות את כל המידע על אודות דרכי ההתקשרות עימו (טלפון, פקס, דואר אלקטרוני), לרבות באמצעות הרשתות החברתיות (פייסבוק, טוויטר ועוד).

(ד) מידע הנוגע לפעילות שהפירמות מבצעות במידע האישי אודות הצרכנים - המציאות הטכנולוגית הנוכחית המאפשרת לספקים לאסוף מידע אודות הצרכנים, היא חלק בלתי נפרד מעסקאות צרכניות המתבצעות כיום בשווקים הדיגיטליים. חוק הגנת הצרכן אינו מטיל חובת גילוי מפורשת המתייחסת לכך.[41]

<u>סיכום ביניים:</u> סקירת המשפט המצוי בישראל חושפת כי המצב הרגולטורי הקיים הוא חלקי וחסר. חסרות הוראות חוק ברורות לאסדרת חובות זיהוי וגילוי מידע שתוטלנה על ספקים של מוצרי IoT. אף שניתן לעיתים לגזור חובות גילוי ספציפיות מתוך עקרונות רחבים המעוגנים בדין הכללי (חובות גילוי כלליות לצד עקרון תום הלב החלים מכח דיני החוזים ודיני הגנת הצרכן), מוצע לייחד פרק ייעודי בחוק הגנת הצרכן לאסדרת נושא חדש וחשוב זה. הטעם לכך נעוץ בשילוב נתונים: מורכבות הנושא הנובעת מאופיו הטכנולוגי; א-סימטריה במידע המוביל לנחיתות צרכנית; לצד הצורך בוודאות העוסקים בענף. להלן נציג המלצות ראשוניות להרחבת טיוטת ההנחיה ולאסדרה.

<u>המלצות</u>

לפי טיוטת ההנחיה שפרסמה הרשות להגנת הצרכן וסחר הוגן, "קמה חובה לגלות לצרכן בטרם הרכישה של מוצר IoT כי מדובר במוצר שעלול להיות מנוצל לרעה על ידי גורם זדוני לצורך ביצוע תקיפת סייבר". בנוסף, לפי ההנחיה המוצעת, חלות חובות גילוי אלה:

- חשיבות החלפת הסיסמא הראשונית;

- הוראות כיצד ניתן להחליף את הסיסמא;

- האם היצרן צפוי לפרסם עדכוני אבטחה;

[41] על אף שספק אם סעיף 7 לחוק הגנת הפרטיות המגדיר את המונח "מאגר מידע" מקיף את כל סוגי המוצרים והשירותים הרלוונטים לאינטרנט של הדברים, יצויין כי תיקון 14 לחוק (שעבר בקריאה ראשונה) תיקן את ההגדרה כך שתהיה רחבה יותר (גם הגדרה זו לא ברור אם מקיפה את כל המוצרים והשירותים הרלוונטים).

- משך הזמן שבו היצרן צפוי לפרסם עדכוני אבטחה למוצר (End of Life);

- במקרה והעדכון אינו אוטומטי, כיצד ניתן להתקין עדכוני אבטחה;

- חובות גילוי ספציפיות נוספות לשיקול דעתם של היצרן והיבואן בהתאם לאופי המוצר ורמת הסיכון הנובעת מהשימוש בו.

לדעתנו, וברוח הרגולציה המתגבשת בעולם המערבי, יש מקום לחדד את חובות הגילוי המוטלות על ספק במסגרת ההנחיה, במספר היבטים:

ראשית, ראוי לדעתנו כי אופן ביצוע חובת הגילוי יובהר באופן שאינו משתמע לשתי פנים לספקים שאמורים לגלות את המידע, תוך מזעור האפשרויות לטשטש ולהתחכם:

רצוי להנחות את הספקים לאמץ נוסח ברור ומפורש (גם באמצעות דוגמא); להנחות לגבי אופן הגילוי (בכתב); ולציין כי הגילוי ייעשה בשלב הצגת המוצר והמוקדם ביותר האפשרי. מטרת ההבהרה היא לקדם וודאות לגבי חובת הגילוי ודרך ביצועה, אינטרס שהוא לטובת הצרכן כמו גם לטובת הספק. מוצע לשקול לעניין זה הנחיה מפורשת להצמדת תוויות המכילות מידע לצרכן, באופן דומה להנחיה במסגרת רגולציות בעולם ולהצעות המועלות בספרות המחקרית.

שנית, על חובת הגילוי לכלול התייחסות מפורשת למשך הזמן בו תינתן תמיכה טכנית למכשיר, פירוט של תקלות מערכתיות ומה נעשה כדי למונען ויצוין מי הוא הגוף האחראי לפגמים או תקלות במכשיר[42] לרבות ציון כל דרכי ההתקשרות עימו.

שלישית, ראוי כי חובת הגילוי של הספק תכלול התייחסות לא רק לעצם קיומו של סיכון הפגיעה בפרטיות אלא גם לאופי הפגיעה והנזק שעלול להיגרם. בהקשר זה מוצע כי יידרש גילוי מהספק גם לגבי מיקום ואופן אחסון המידע על אודות הפרט, סוגי המידע הנאסף עליו, מטרת האיסוף, והשימוש הנעשה בו[43].

רביעית, מוצרי IoT עשויים להיות שונים זה מזה בתכונות רבות כגון מטרת המוצר, כמות המידע הנאסף וסוגו, ורמת הסיכון למשתמש. סעיף 2(5) לחוק עקרונות האסדרה, תשפ"ב-2021 קובע כי "*האסדרה נקבעת, במידת האפשר, בהתחשב בסוגי הגורמים שהיא חלה עליהם ומאפייניהם, ובכלל זה גודלם, היקף פעילותם או מידת הסיכון הכרוכה באותה פעילות...*". נציע כי בנוסף לחובת גילוי בסיסית בה חייבים כל הספקים, בהיווצר תנאים מסוימים של סיכון מוגבר, תוטל על הספקים חובת גילוי מוגברת, שתכלול מידע נוסף שיהיה על הספק לגלות לצרכן. חובה זו תהיה תלויה בין השאר במאפייני השירות או המוצר, בזהות הלקוח, ובמטרת הרכישה (רשימה שאינה סגורה), כך שתשקף את הסיכון המוגבר שבמוצר (דוגמא לכך יכולה להיות שימוש במוצר שהסיכון של פריצה לתוכו עלול לסכן בריאותו של אדם. הצעה זו משקפת את העיקרון המשפטי שהיקף חובת הגילוי תלוי ביתרון היחסי שיש לאחד

[42] האינטרנט של הדברים (IOT) בישראל - תועלות, אתגרים והמלצות מדיניות, איגוד האינטרנט הישראלי, פברואר 2022
[43] האינטרנט של הדברים (IOT) בישראל - תועלות, אתגרים והמלצות מדיניות, איגוד האינטרנט הישראלי, פברואר 2022

הצדדים בגישה למידע ולנתונים, כך שככל שקיים יתרון יחסי גדול יותר לאחד הצדדים, כך תגדל חובת הגילוי החלה עליו.[44] עיקרון זה חוזר על עצמו בפסיקה ואנו ממליצות להביאו לידיעת הספקים.

לבסוף, בראיה רחבה וצופת עתיד, אנו מציעות כי תישקל הוספת פרק בחוק הגנת הצרכן אשר יטפל באופן ספציפי בעסקאות במוצרי IoT במסגרת פרק ג' לחוק ("הוראות לעניין סוגים של עסקאות"). פרק זה יכלול חובות גילוי מפורשות, כמפורט לעיל.

נשמח לעמוד לרשותכם בכל שאלה.

בכבוד רב ובברכה,

השופטת בדימוס ד"ר איריס סורוקר

ד"ר דנה נייער

[44] ע"א 7730/09 ניסים כהן נ' מבני גזית (2000) בע"מ; ע"א 17501-10-16 הולמס פלייס אינטרנשיונל בע"מ נ' גלי הקטיפה בע"מ

מרכז רנה ומאיר חת לחקר התחרות והרגולציה, המסלול האקדמי – המכללה למינהל
טלפון: 03-9634104 | דוא"ל המרכז: hethcenter@colman.ac.il
רח' אלי ויזל 2, ראשון לציון | בקרו אותנו באתר: www.colman.ac.il/heth_center
עמוד הפייסבוק: https://www.facebook.com/hethcenter/

נספח א


Security & Privacy Overview
Smart Security Camera, NS200
Firmware version 2.5.1: updated on: 6/15/2019
The device was manufactured in: United States
Casa
Security Mechanisms
Security updates
Automatic (available untill 1/1/2022)
Access control
Password, Factory default, User-changeable, Multiple user accounts are allowed
Data Practices
Sensor data collection
Video
Audio
Purpose
Providing device functions, research
Providing device functions, research
Data stored on device
Identified
Identified
Data stored on cloud
Identified, Option to delete
Identified, Option to delete
Shared with
Manufacturer
Manufacturer
Sold to
Not sold
Not sold
Other collected data
Presence, Temperature, Carbon monoxide, Usage information, User-entered information
Privacy policy
www.NS200.example.com/privacypolicy
More Information
Detailed Security & Privacy Label:
www.iotsecurityprivacy.org/labels

Security & Privacy Details

Smart Security Camera, NS200
Firmware version 2.5.1, updated on: 6/15/2019
The device was manufactured in: United States

Casa

Security Mechanisms

Security updates	Automatic (available until 1/1/2022)
Access control	Password, Factory default, User-changeable, Multiple user accounts are allowed
Security oversight	Audits performed by internal security auditors
Ports and protocols	www.NS200.example.com/port
Hardware safety	www.NS200.example.com/hwsafety
Software safety	www.NS200.example.com/swsafety
Personal safety	www.NS200.example.com/usersafety
Vulnarability disclosure and management	www.NS200.example.com/vulreport
Software and hardware composition list	www.NS200.example.com/BOM
Encryption and key management	www.NS200.example.com/key

Data Practices

Sensor data collection	Video	Audio	Presence	Temperature	Carbon Monoxide
Collection frequency	When user requests it	Continuous, Adjustable	Periodic, Option to opt-out	Continuous, Option to opt-in	Continuous, Option to opt-out
Purpose	Providing device functions, research	Providing device functions, research	Providing device functions	Providing device functions	Providing device functions
Data stored on device	Identified	Identified	De-identified	De-identified	De-identified
Local data retention time	Up to a month	Up to a month	Up to a year	Up to a year	Up to a year
Data stored on cloud	Identified, Option to delete	Identified, Option to delete	No cloud storage	De-identified	De-identified
Cloud data retention time	Up to a month	Up to a month	No cloud storage	Up to a month	Up to a month
Shared with	Manufacturer	Manufacturer	Not shared	Manufacturer, Third-party	Third-party, option to opt-out
Sharing frequency	Periodic, Adjustable	Periodic, Adjustable	Not shared	Continuous	Continuous
Sold to	Not sold	Not sold	Not sold	Third-party	Third-party, Option to opt-out

Other collected data	Usage information, User-entered information
Data linkage	Data may be linked with internal and external data sources
What could be inferred from user's data	No data inference
Special data handling practices for children	Yes
In compliance with	GDPR, ISO27001
Privacy policy	www.NS200.example.com/privacypolicy

More Information

Call Casa with your questions at	412-313-2793 (24/7 support)
Functionality with no internet	Limited functionality on offline mode
Functionality with no data processing	Limited functionality on dumb mode
Physical actuations and triggers	Device blinks when motion is detected
Compatible platforms	Amazon Alexa

מרכז רנה ומאיר חת לחקר התחרות והרגולציה, המסלול האקדמי – המכללה למינהל
טלפון: 03-9634104 | דוא"ל המרכז: hethcenter@colman.ac.il
רח' אלי ויזל 2, ראשון לציון | בקרו אותנו באתר: www.colman.ac.il/heth_center
עמוד הפייסבוק: https://www.facebook.com/hethcenter/