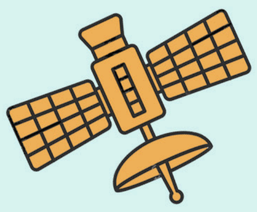
מעקב במרחב הציבורי

1. מעקב לווייני

צילומי לווין קיימים משנות ה-50. **כיום בכל רגע נתון ישנם כמעט 10,000 לווייניים במסלול מעל כדור הארץ** – לחלקם יכולות צילום מתקדמות. בעוד רבים מהם מיועדים למטרות מדעיות, בחלקם נעשה שימוש צבאי ומודיעיני. ישנם לווייניים שעשויים לזהות בניין, סוג רכב, או אדם בודד בתוך התקהלות. כיום תמונות שצולמו מלווין עדיין לא ברורות מספיק או לא ממוקמות בזווית הנכונה כדי לעבוד עם טכנולוגיית זיהוי פנים או קריאת לוחיות רישוי, אבל יתכן שבעתיד הלא רחוק הטכנולוגיה תתגבר גם על המרחק הזה. לעומת זאת **לווייניים מאפשרים מעקב על ידי מתן אפשרות לממשלות, וארגוני מודיעין ומסוגלים ליירט או להאזין למידע ונתונים המועברים ברשתות בינלאומיות.**

הלווייניים הם הבסיס לג'י.פי.אס Global Positioning System, ובעברית: "מערכת מיקום עולמית". הלוויין קולט את המידע מהמקלטים שאותם אנו מחזיקים, לרוב טלפונים סלולריים, וכך מחשב את המיקום שלנו. על בסיס הג'י.פי.אס התפתחו יישומים שונים, לרבות מערכות ניווט הזמינות לכולנו (וויז, גוגל מפות). המערכות הללו משתמשות בנתונים לעקוב אחרי מיקום ותנועה של בעלי המכשירים.



2. רחפנים

רחפן הוא כלי טיס זעיר, נשלט מרחוק, בעל יכולות צילום והקלטה שהופכות אותו לאמצעי מעקב יעיל וחודרני במיוחד, המסוגל לאסוף מידע רגיש בכל עת, גם מבעד לקירות ומכשולים, ואף לייצר תמונת מצב עדכנית בזמן אמת. בשל גודלו ומשקלו הקל, ניתן הרחפן לתמרון ובזכות גובה הטיסה הנמוך שלו אפשר לקבל דרכו תצלומי אוויר איכותיים ברזולוציה גבוהה ביותר (1 ס"מ לפיקסל).

בנוסף לשימוש ברחפנים צבאיים למטרות ביון, מעקב ולוחמה, בתוך ישראל ומעבר לגבולה, גופים ציבוריים בישראל – **משרדי ממשלה, רשויות מקומיות, משטרה – החלו להשתמש ברחפנים למטרות אזרחיות של עיבוי חקירה, שיטור ואכיפה .**

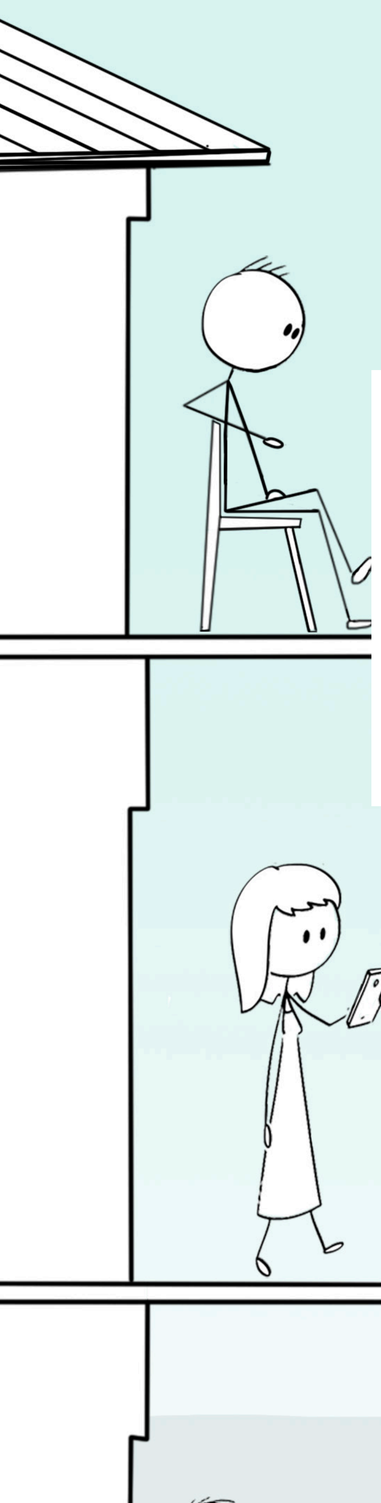
בימי הקורונה נעשה שימוש ברחפנים כאמצעי שיטור ואכיפת בידוד. יש עדויות מרחבי העולם על שימוש ברחפן המצויד במצלמת אינפרה-אדום שמאפשרת לזהות אנשים עם חום גבוה, ורחפנים עם מערכת זיהוי מרחוק של נתוני בריאות כמו חום, קצב לב וקצב נשימה המאתרים חולים.

כאשר מבחינים ברחפן אין לדעת מה תחום הכיסוי שלו ואילו טכנולוגיות מותקנות עליו, לאיזו מטרה ובידי מי. בנסיבות אלה, ככל שתגדל תפוצת הרחפנים, כך תלך ותעמיק בציבור התחושה כי פוטנציאלית הכול נתונים למעקב בכל מקום ובכל שעה.

3. אנטנות סלולריות

מגדלי אנטנות סלולריים קולטים מידע שלנו כל הזמן – נתונים כמו מיקום המכשיר, מטא-נתונים כמו שיחות שבוצעו, משך השיחה, תוכן שיחות והודעות טקסט לא מוצפנות. **על פי החוק, מידע זה, שמתוחזק על ידי חברות הטלקום, יכול להינתן למשטרה ורשויות אחרות במידה והשיגו צו בית משפט.** שימוש באפליקציות תקשורת מוצפנות, (ראו פוסטר 3), או השארת הטלפון הסלולרי בבית הן כמה דרכים למנוע מעקב מסוג זה.

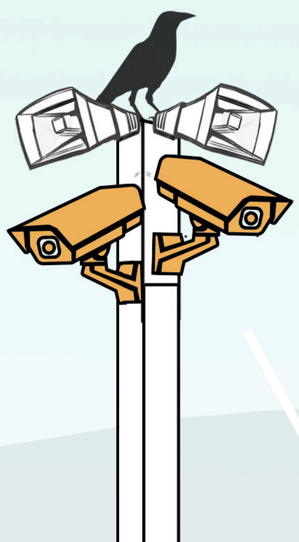
במרץ 2020 החליטה ממשלת ישראל להסמיך את השב"כ לבצע מעקב מגעים ולזהות מיקומים של חולי קורונה, ושל כל מי שבא עמם במגע. כך נחשפה תכנית המעקבים של השב"כ (המכונה "הכלי"). התברר ש**השב"כ מקבל באופן רציף וגורף מידע מחברות הסלולר והאינטרנט שלנו, מידע שמאפשר לו לדעת בתוך שעות איפה היינו, עם מי נפגשנו ולכמה זמן, והאם היינו ליד מישהו במרחק קרוב וליותר מ-15 דקות. מאגר נתוני התקשורת שבידי השב"כ נאסף ללא צו משפטי וכמעט ואין עליו פיקוח חיצוני.**



4. מצלמות מעקב במרחב הציבורי

מצלמות מעקב הן אחת הטכנולוגיות הנפוצות והמוכרות ביותר המשמשות כדי לצפות בנו בזמן שאנו נעים בחיי היומיום שלנו. הן עלולות לפגוע בנו בכך שהן מאפשרות לגורמי שלטון רבים תיעוד של החיים בציבור – לאן אנו הולכים, עם מי אנו נפגשים, באיזה אירועים אנו משתתפים ואפילו עם איזה רופאים או עורכי דין אנחנו מתייעצים.

מצלמות מעקב, ציבוריות או פרטיות, נמצאות בכל מקום ברוב הערים בישראל. למרות שיש דיון נרחב בנושא, ושטרם התקבלה הוכחה מובהקת לכך שמצלמות מעקב מפחיתות את הפשיעה, הרי שגופים ממשלתיים, רשויות מקומיות, ארגונים ואנשים פרטיים ממשיכים להציב מצלמות נוספות, ולצייד אותן ביכולות פולשניות יותר. דגמים מסוימים יכולים להיות מצוידים בתוכנת זיהוי פנים או יכולות אנליטיות שונות. מכיוון ש**רבות מהמצלמות גם מחוברות ישירות לאינטרנט, פצחנים (האקרים) כבר זיהו אותן כמטרות קלות לפריצה.** למצלמה יש זיכרון. הוידאו מוקלט ונשמר, המידע נוסף למאגר, נלמד ומנותח. המידע מהצלמות משותף לרוב עם גורמים אחרים, הן פרטיים (תאגידים) והן ציבוריים (גופים ממשלתיים).



5. זיהוי פנים

זיהוי פנים היא שיטה לזיהוי או אימות הזהות של אדם דרך הפנים שלו, בדיעבד או דרך המצלמה בזמן אמת. טכנולוגיות זיהוי פנים מבוססות על תהליך עיבוד מידע ביומטרי, ונתונים אישיים על בסיס מאגר פנים קיים. כלומר, האלגוריתם שנקבע ככזה מאתר האם תווי פנים של פלוני זהים לאלו המצויים במאגר, וקובע את המענה לשאלה כהכרעה ביחס לרמת הדיוק שנתבקשה. אם הפנים אינם במאגר המערכת יכולה עדיין לעקוב אחרי התנועה של הדמות.

הפנים שלנו הם גורם זיהוי ייחודי שאיננו יכולים להשאיר בבית, או להחליף כמו תעודה זהות גנובה או סיסמה שנפרצה. **טכנולוגיה זאת מאפשרת מעקב המוני סמוי אחר המקומות שאנו פוקדים, אנשים שאנו פוגשים, ואפילו המצב הרגשי שלנו. ישנן הטיות במערכות ביומטריות הנוגעות לגזע ואף למגדר**, ומערכות זיהוי פנים יכולות להיות מועדות לטעות, מה שעלול לגרום לאנשים להיחשד בפשעים שלא ביצעו.

על פי פרסומים בעיתונות, משטרת ישראל רכשה מערכת לזיהוי פנים והיא ביקשה להיות רשאית להפעיל אותה ללא מסגרת חקיקה מסודרת. הבקשה סורבה לבסוף, אך בהינתן שהכלי קיים והוא תפעולי ניתן להניח שבידי המשטרה כבר קיים מאגר פנימי של תצלומי פנים של אזרחים.

מעקב במרחב הפרטי

1. מעקב אחר תנועה באינטרנט – תאגידי

אנו משאירים את העקבות הדיגיטליים שלנו בכל מקום אליו אנו הולכים. כל מקום באינטרנט בו אנו מבקרים, כל חיפוש, כל מודעה או ידיעה שלוחצים עליה, אוהבים או משתפים, מנוטר בקפידה, מתועד ומנותח. חברות טכנולוגיה עוקבות אחר ההתנהגות המקוונת שלנו כדי למכור לנו מוצרים ושירותים, ללמוד ולעצב את ההתנהגות שלנו גם כדי למכור את הדאטה שלנו לגורמיים מסחריים נוספים.

עוגיות, קוקיס, זה שם נחמד נורא לקבצים קטנים הנשארים על המחשב שלכם לאחר ששוטטתם באתרים – קבצים קטנים המכילים מידע על המכשיר שלך, איך אתה גולש וכן הלאה. אתרי אינטרנט מסחריים הם לא היחידים שיציעו לכם 'עוגיות' כדי לאסוף אליהם את נתוני המשתמשים. גם המדינה עושה זאת ואף משתפת פעולה עם תאגידים מסחריים באיסוף הנתונים, כך למשל, אתרים ממשלתיים מטמיעים קבצי מעקב (Cookies/Trackers) של חברות צד-שלישי (דוגמת גוגל). החדשות הטובות הן שהעוגיות נעלמות. גוגל הודיעה שהיא לא תעקוב עם קוקיס בכרום החל משנת 2022 (אם כי זה נדחה עד 2023).

2. מעקב אחר תנועה באינטרנט – ממשלתי

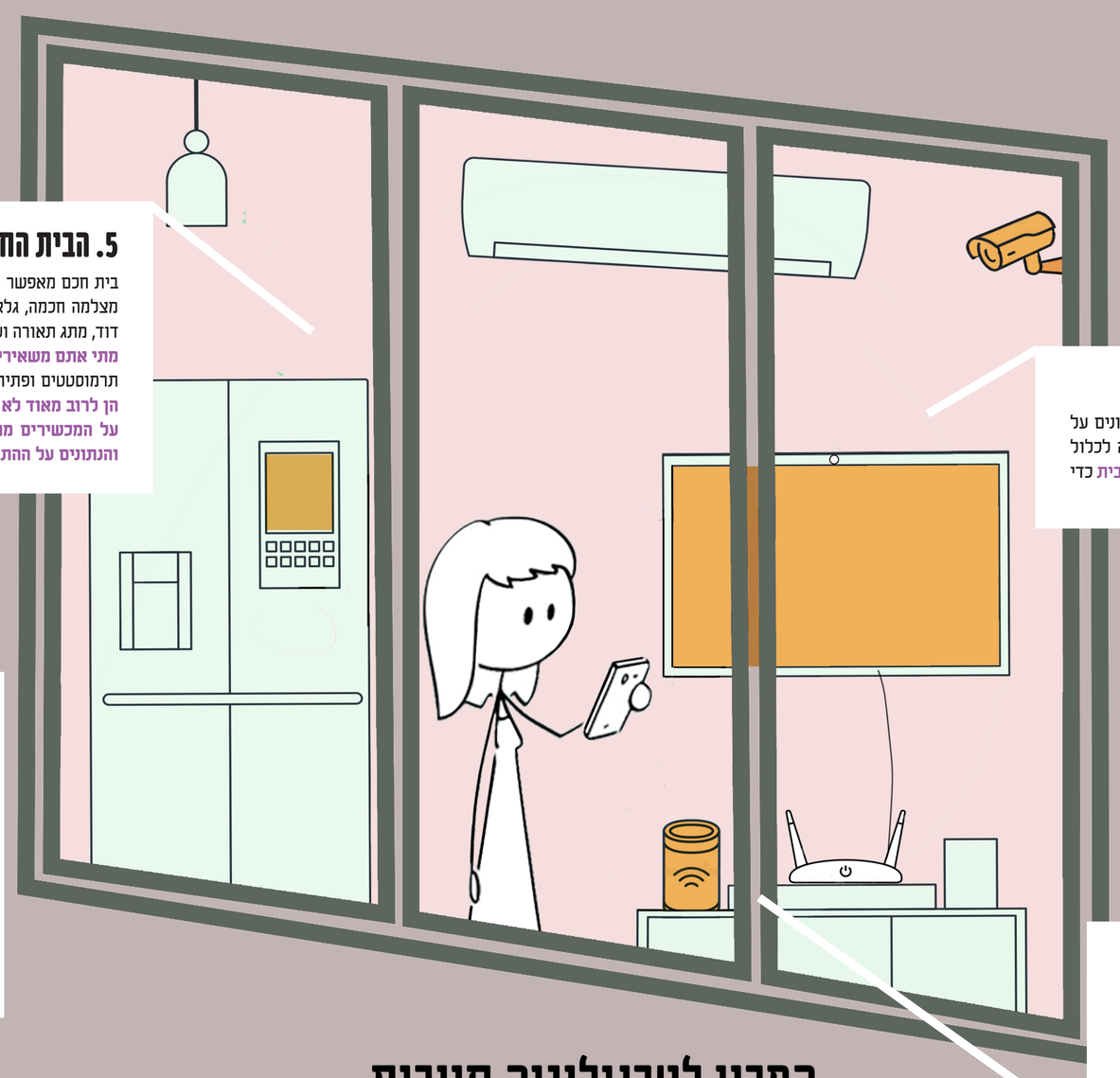
דרך ניטור הודעות דוא"ל כשהן נעות ברחבי האינטרנט, מעקב אחר הדפדפן והיסטוריית החיפושים, ואפילו הקלדה בזמן אמת, עוקבות סוכנויות ממשלתיות אחרי תעבורת האינטרנט. חלק גדול מהמידע הזה יכול להגיע ישירות מחברות האינטרנט והטלקום שאתם משתמשים בהן, באמצעות הסכמים בין חברות אלה לסוכנויות ממשלתיות. **רשויות אכיפת החוק המקומיות יכולים לפנות לחברות הטכנולוגיה הגדולות (כגון פייסבוק וגוגל) לקבל את המידע דרך צו בית משפט והתאגידים הפרטיים יכולים להידרש להעביר את כל המידע שלכם** (התכתבויות, תמונות, חיפושים ועוד) למשטרה. התאגידים הטכנולוגיים המובילים (גוגל, מטא, מיקרופוספט, אפל, אמזון) הודו בפומבי על העברת נתוני לקוחות לממשלה. סוכנויות ממשלתיות גם קונות דאטה מחברות פרטיות.

3. רומבה iRobot

בזמן ששואב האבק הרובוטי מנקה לכם את הבית הוא אוסף דאטה ולומד להכיר את הבית – גודל הבית, מיקום וגודל המטבח, חדר הילדים, רהיטים שיש בבית (וכמה הם חדשים). המידע הזה הוא מכרה זהב עבור חברות הטכנולוגיה, שמטרתן העיקרית היא למכור לנו יותר מוצרים ושירותים. **חברת אמזון רכשה את חברת iRobot בסכום של 1.7 מיליארד דולר בגלל המידע שבידיה על פנים הבית.** וכך יש בידיה כיום רובוט שעוקב אחר מבנה הבית שלכם, הסלון, המחסן, רהיטים וצעצועים, הוא יודע האם יש לכם חיות מחמד ובכלל איך אתם חיים.

4. מצלמות אבטחה

מצלמות אבטחה פרטיות, נמכרות היום בזול לכל צרכן והופכות אט אט לרשתות כלל עולמיות. בניגוד למצלמות אבטחה מסורתיות ששמרו על הצילומים בכונן מקומי של המשתמש, **מצלמות האבטחה היום מחוברות לאינטרנט ומאחסנות את הצילומים בשרתי חברת המצלמות.** למעשה כשהמצלמה מחוברת לרשת היא מאפשרת גישה נוחה לרבים: בין אם מדובר שמשטרה וסוכנויות ממשלתיות, סוחרי מידע מסחריים וגם פושעים דרך האקינג או מדובר בתאגידי ענק אמריקאים כמו אמזון או חברות סיניות כמו Hikvision (חברת המעקב הגדולה בעולם).



5. הבית החכם

בית חכם מאפשר לנהל מגוון גלאים ומתגים חכמים ולעקוב מרחוק אחר הנעשה בבית. מצלמה חכמה, גלאי מזגן, גלאי הצפה, גלאי תנועה, גלאי דלת/ חלון, מתג תריס, מתג דוד, מתג תאורה ועוד. **מערכות הבית החכם יכולות לעקוב אחריכם, מתי אתם בבית, מתי אתם משאירים את האורות דולקים, ובכלל מי בבית ומתי.** מכשירי בית חכם כמו תרמוסטטים ופתיחת דלת מהנייד עשויים להיות מאוד נוחים, אבל **הטכנולוגיות הללו הן לרוב מאוד לא בטוחות – התקפות סייבר, השתלת מכשירי מעקב או השתלטות על המכשירים מתרחשים בתדירות ביישומי בית חכם. בנוסף, אין שום רגולציה והנתונים על ההתנהגות שלכם יכולים להימכר לכל המעוניין.**

6. הטלוויזיה החכמה

כשאתם צופים בטלוויזיה חכמה היא צופה בכם, אוספת נתונים על הרגלי הצפייה שלכם, ועוד. הטלוויזיה החכמה שלכם עשויה לכלול גם מצלמה חכמה ומיקרופון – ש**רואים ושומעים מה קורה בבית** כדי לעזור באיסוף נתונים.

7. עוזר.ת דיגיטלי.ת

העוזרת הדיגיטלי.ת (כדוגמת אלכסה של אמזון, Google Assistant או סירי של אפל) מבינה פקודות קוליות ומבצעת משימות עבורכם אבל גם **מקשיבה ויכולה להקליט את כל השיחות הפרטיות שלכם ואת כל מה שקורה בבית.** יש עוזר.ת גם עם מצלמה.

8. בית משותף

בבתים משותפים רבים יש שימוש גובר במצלמות אבטחה ובאמצעים דיגיטליים לניהול הבניין. **אפליקציות לניהול הבניין למשל, שמנסות בעיקרן לשפר את חוויית המשתמש בבית,** להגביר שקיפות וזמינות ולייעל את הגבייה, **אוספות מידע רגיש ופרטי על הדיירים.** הדאטה הזו נשמרת לרוב אצל חברות הניהול, וגם מידע זה לא מוסדר בשום צורה.

מצלמות, שמותקנות בטענה שנועדו להגביר את הביטחון, בפועל, אוספות מידע על הדיירים ועל מי שמבקר בבנין. יש בניינים עם חדרי בקרה, מצלמות שמכוונות לכל נקודה – בכניסה, בקומות, בכניסה לחניון, בחדר הכושר. **המצלמות נהפכו לכלי פנימי לבקרה ואכיפה.**

המכון לטכנולוגיה חיובית

למידע נוסף: www.positive-tech.net

מעקב סלולרי

1. מעקב סלולרי

הטלפון הסלולרי מאפשר **מעקב אחרי מטא-נתונים של שיחות** (מי דיבר עם מי ולכמה זמן?), **קריאת התוכן של הודעות טקסט לא מוצפנות, מעקב אחר הרגלי שימוש באינטרנט, מיקום, אנשי קשר** בקיצור שפע של מידע שנאסף, מאוחסן ומופץ על ידי המכשיר כל הזמן. לספקי השירות (סלקום, פרטנר, פלאפון וכו') ישנם נתונים אלה והם משתפים בהם גורמים ממשלתיים ומסחריים לפי הסכמים.

2. מעקב מאפליקציות

חלק מ**האפליקציות שהורדתם לנייד ואתם משתמשים בהן עלולות למעשה לסכן אתכם.** אפליקציות רבות אוספות מידע ומטא מידע מהמכשיר (הרי נתתם להם אישור כשהורדתם אותם!) ומוכרות אותו לסוחרי מידע. לאחרונה התפרסם שממשלת ארה"ב רוכשת נתונים זמינים מאפליקציות שאנשים הורידו לטלפונים שלהם. כך למשל רכש משרד ההגנה של ארצות הברית מידע שנאסף מאפליקציות תפילה שפותחו עבור מוסלמים. שימו לב לגבי הרשאות של כל אפליקציה, ו**כבו הרשאות שאינן נדרשות כדי שהאפליקציה תפעל כראוי.**

3. מעקב מיקום

יכולת מעקב בולטת של טלפונים ניידים היא הדרך שבה הם מכריזים על מקום ההימצאות שלכם כל היום (וכל הלילה) דרך האותות שהם משדרים. ממגדלים סלולרים, ממעקב Wi-Fi ו-Bluetooth וממידע על מיקום מאפליקציות וגלישה באינטרנט באמצעות הג'י.פי. אס במכשיר. במערכת ההפעלה של כל מכשיר קיימים "שירותי מיקום". אפליקציות (כגון מפות) יכולות לבקש מהטלפון מידע על מיקום זה ולהשתמש בו כדי לספק שירותים המבוססים על מיקום. מודל ההרשאות במכשירים עדכניים מבקש רשות כדי שיישומים יבקשו להשתמש במיקום. עם זאת, יישומים מסוימים יכולים להיות אגרסיביים יותר מאחרים בבקשת שימוש בשירותי מיקום. חלק מהאפליקציות הללו ישדרו את מיקומנו ברשת לספק השירות, אשר בתורו מספק את המידע דרך אפליקציה לצדדים שלישיים שאיתם הם עשויים לעקוב אחריך. חלק מהטלפונים החכמים יתנו לך איזושהי שליטה על היכולות של אפליקציות לגלות את המיקום הפיזי; **נוהל פרטיות טוב הוא לנסות להגביל אילו אפליקציות יכולות לראות מידע זה, ולכל הפחות לוודא שהמיקום שלכם ישותף רק עם אפליקציות אמינות.** אפשר גם לכבות את שירותי המיקום בנייד שלכם.

4. מעקב רשתות חברתית

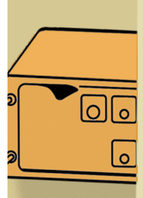
רשתות חברתיות הן בין רשתות המידע והאתרים הפופולריים ביותר באינטרנט. לפייסבוק ולטיקטוק יש יותר ממיליארד משתמשים, ולאינסטגרם וטוויטר יש מאות מיליוני משתמשים כל אחת. רשתות חברתיות בנויות על הרעיון של שיתוף תוכן, פוסטים, תמונות ומידע אישי. כיום הם גם מקום מרכזי לארגון אירועים ולדיון ציבורי, כולל התארגנות פוליטיות. בעוד רבים משתמשים ברשתות החברתיות כדי לתקשר ולשתף תמונות, רעיונות וסוגים אחרים של מידע עם חברים ועוקבים, המטרה העיקרית של תאגידי המדיה חברתית היא להשתמש בכל הנתונים האלה כדי ליצור פרופילים אישיים שניתן להשתמש בהם וכך להציג למשתמשים פרסומות ממוקדות. הפרופילים הללו הם בעלי ערך מודיעיני עצום, ומאפשרים יכולות פיקוח, תמרון ושליטה. יכולות אלו נבנו לשימושים מסחריים, אבל גורמים **פוליטיים, מדינות זרות, רשויות אכיפת חוק וסוכנויות מודיעין עושות בהם שימוש הולך וגובר למניפולציות, להפצת פייק נוז, והפצת דעות קיצוניות שגורמות לניכור בין אנשים.**

האפליקציות של הרשתות החברתיות פולשניות ביותר ועדיף לגלוש ברשתות החברתיות דרך הדפדפן.

5. מעקב המדיה החברתית מחוץ לפלטפורמות

כשאנחנו משתמשים ברשתות חברתיות אנו יודעים שעוקבים אחרינו, ומבחינת התאגידים הרי עשינו עסקה – המידע שלנו תמורת השימוש בפלטפורמה. **אבל הרשתות החברתיות עוקבות אחרינו גם כשאנחנו לא נמצאים בהן.** מטא הענקית החברתית (פייסבוק, אינסטגרם, וווטסאפ) אוספת נתונים מכולם בכל רחבי האינטרנט וגם מאנשים שאין להם חשבון פייסבוק. לדוגמה, כאשר אתם מנווטים ברחבי האינטרנט, אתרים המשתמשים בפיקסל הפרסום של פייסבוק או ממשקי API חברתי אחרים שולחים נתונים על אותם ביקורים באתר בחזרה לענקית החברתית .הנתונים האלה על כל מי שמבקר באתרים אלה נאספים, בין אם הגולשים רשומים או לא. הזרועות של מטא משתרעות על פני אתרים ושירותים אחרים, לתוך האפליקציות השונות בהן אתם משתמש בטלפון, ואפילו למקומות שבהם אתם מבקרים פיזית בעולם האמיתי.

פתיחת קישור מתוך הפלטפורמה: פתחתן קישור בפייסבוק או אינסטגרם? מטא יכולה לעקוב אחריכן, ללא הסכמה. בכל פעם שפותחים קישור מתוך אפליקציות אינסטגרם ופייסבוק, חברת מטא מזריקה קוד שמאפשר לה לעקוב אחר כל הנעשה בדפדפן שנפתח מתוך האפליקציות שלה, לרבות איסוף סיסמאות וכרטיסי אשראי (כדי להימנע מהמעקב מומלץ להעתיק את הקישור ולפתוח אותו מחוץ לאפליקציה). לא רק מטא, גם טיקטוק מזריקה קוד לדפדפן הפנימי שלה, שגורם לכך שכל המידע נאסף. זהו חלק מאסטרטגיית איסוף המידע המאפיינת את ענקיות הטכנולוגיה שעוקבות אחרינו.



6. מעקב השתתפותי

מיליארדי משתמשים בעולם משתפים מרצונם ובפרהסיה בחוויות, בדעות, בהעדפות ובמידע ייחודי על עצמם ברשתות החברתיות. נורמות חברתיות נאכפות לא רק באמצעות "האח הגדול" (מעקב מלמעלה) אלא גם באמצעות פיקוח חברתי רוחבי (כולנו "מוזמנים להיות מרגלים"). **ברשתות החברתיות אנשים נדרשים לתרום למעקב של עצמם באופן פעיל, ולתרום מרצונם לרשתות ולמאגרי המידע שלהם.** עצם ההשתתפות לא הופכת את כולם לשווים ואינה משנה את מבני הכוח, יתרה מזו, יותר השתתפות מאפשרת יותר מעקב, שמאפשר את השליטה על המשתתפים, ומאפשר לשלטון ולתאגידים להרחיב את יכולת המעקב אחריהם.

7. מעקב שלטוני ברשתות חברתיות

סוכנויות שונות של השלטון מנהלות מעקב אחר רשתות חברתיות במספר דרכים שונות – משליחת סוכנים לחדור לקבוצות פייסבוק פוליטיות או מארגנות מחאה, שימוש בחשבונות מזויפים כדי להתגנב לקבוצות מדיה חברתית עם גישה סגורה ועד לאיסוף המוני וניטור של האשטאגים או פוסטים במיקום גיאוגרפי בסיוע בינה מלאכותית.

ישנם מעט חוקים המסדירים את השימוש של אכיפת החוק בניטור מדיה חברתית.

8. אפליקציות מסרים מידיים

לשלוח הודעה בתוכנה לא מוצפנת זה כמו לשלוח גלויה. תחשבו שכל אחד יכול לקרוא את התוכן שלה. אפליקציות מסרים מיידים חינמיות , כגון וווטסאפ, מסנג'ר, טלגרם וסיגנל מאפשרות העברת הודעות מוצפנות מקצה לקצה דרך האינטרנט. אבל יש הבדלים ביניהם, ונשאלת השאלה על איזה שרות הודעות אפשר לסמוך.

הצפנה מקצה לקצה (שדואגת שרק האדם שאליו אתם שולחים את ההודעות יכול באמת לקרוא אותן) יכולה להגן עליכם מפני מעקב של השלטון, האקרים ופלטפורמת ההודעות עצמה. אבל כל האפליקציות האלה עשויות לבצע שינויים בתוכנה . לדוגמה, **וווטסאפ** (של חברת מטא), האפליקציה המועדפת על **רוב המשתמשים בארץ, אמנם בנתה הצפנה מקצה לקצה בגרסאות העדכניות ביותר שלה, אך היא שינתה את מדיניות הפרטיות שלה כדי לאפשר שיתוף של מגוון רחב של נתונים – כגון מספרי טלפון, שמות פרופילים, סטטוס, נתוני מכשיר, כתובת IP, נתוני מיקום, ומידע על תדירות שליחת הודעות והנמענים שלהן.** מסנג'ר של מטא וטלגרם מציעים הצפנה מקצה לקצה, אבל לא כברירת מחדל.

האפליקציות הללו טוענות שההודעות מוצפנות מקצה לקצה, אולם מכיוון שמדובר בתוכנות קוד סגור שאין לנו גישה אליהן, אי אפשר לבדוק את הטענה הזאת.

מה הצפנה מקצה לקצה לא עושה

הצפנה מקצה לקצה מגינה רק על תוכן התקשורת שלך, ואינה מגנה על המטא נתונים שלך, הכוללים, למשל, עם מי אתם מתקשרים (לאיזה מספר) ומתי, ובאיזה מכשיר אתמשתמשים. מידע על המיקום שלך הוא גם מטא נתונים והן שומרות אותו לנצח.

מומחי פרטיות ממליצים על סיגנל (signal). אפליקציה הכתובה כקוד פתוח אשר מצפינה את ההודעות מקצה לקצה, ולא שומרת מידע או מטא־מידע.

במקרים שבהם רשויות אכיפה בארה"ב הוציאו צו משפטי שהורה לסיגנל לחשוף מידע על התקשורת בחשבון מסוים, הן קיבלו בחזרה דף ריק, כיוון ששום מידע לא נשמר אצל סיגנל מלכתחילה. אפליקציית המסרים Element מציעה אחסון מבוזר, כך שנתוני ההודעות אינם מוחזקים במקום אחד על ידי חברה אחת – אפשר אפילו להגדיר שרת אישי. אף אחד לא יכול להגיע לנתוני המשתמש אלא אם כן הם הנמענים המיועדים להודעות שלך – אפילו לא הצוות של החברה.

עוד סוגי מעקב:

- מעקב פיננסי: כרטיסי אשראי וכרטיסי מועדון
- מעקב בריאות: עזרים רפואיים כמו קוצבי לב ומד סוכר
- מעקב שעוני ספורט וכושר
- מעקב אפליקציות מחזור והריון
- מעקב דרך רכבים חכמים
- רוגלות כמו פגסוס

9. Bluetooth Beacon

ה-Beacon (מגדלור) הוא התקן בלוטות' שמופעל ברדיוס של 30 מטר ומקבל מידע שמשודר מכל המכשירים הסלולרים ברדיוס. הוא יכול לקבל את המיקום שלכם וכל מידע הקשור למכשיר/אפליקציה עם הבלוטות' שלו מופעל. המידע שנאסף באמצעות ה-Beacon משולב לעתים קרובות עם נתונים אישיים אחרים. לדוגמה, **הוא מזהה בחנויות את הסמארטפונים הנמצאים בקרבתו ויכול לשלוח התראות על מבצעים ומסרים מותאמים אישית, המתבססים על פרופיל הקנייה של הצרכן.**

9. סימולטורים של אנטנה סלולרית

טכנולוגיה המחקה מגדל סלולרי (כדוגמת Stingray), וגורמת לטלפונים סלולריים סמוכים להתחבר ולהעביר דרכם נתונים במקום מגדלים לגיטימיים אשר נמצאים בשימוש רשויות החוק וארגוני פשע.

המכון לטכנולוגיה חיובית

למידע נוסף: www.positive-tech.net