

## החלק הנוגע לרקע עובדתי – ביחס להליך המשפטי המתנהל בארה"ב

א. פרטי התביעה:

1. בתאריך 29 לאוקטובר 2019 הוגשה תביעה נזיקית על-ידי החברות Whatsapp ו-Facebook (להלן: "הנתובעות") כנגד החברה הישראלית NSO Group Technologies Limited, וכן כנגד חברת Q Cyber Technologies Limited (בעלת מניות הרוב בחברת NSO) (להלן: "הנתבעות"). התביעה הוגשה בבית המשפט הפדראלי במחוז הצפוני של קליפורניה (תיק מספר 4:19-cv-07123-Northern District of California – להלן: "בית המשפט בקליפורניה").

2. בכתב התביעה (המצורף לבקשה זו ומסומן "נספח א'") נטען, בין היתר, כי הנתבעות יצרו, הפיצו והפעילו תוכנת ריגול כדי ליירט ולהפיק מידע מטלפונים סלולריים או מכשירים אחרים. נטען, כי מוצרי החברה כוללים את תוכנת "פגסוס" - תוכנת ריגול מסוג "סוס טרויאני". נטען, כי תוכנות אלו, לרבות "פגסוס", נועדו להתקין מרחוק ולאפשר גישה מרחוק לשליטה על מידע, לרבות שיחות, הודעות ומיקום – במכשירים ניידיים המשתמשים במערכות ההפעלה של iOS, Android, BlackBerry. כתב התביעה מצייין, כי הנתבעות ניצלו חולשות במערכות ההפעלה ואפליקציות והשתמשו בשיטות בעייתיות נוספות כדי לאפשר את הגישה הנ"ל.

3. נטען, כי בהתאם לפרסומים בתקשורת ולמסמכי NSO, ניתן להתקין את "פגסוס" על טלפון, מבלי שהמשתמש בטלפון ינקוט בכל פעולה שהיא, כגון הקלקה על קישור או הודעה מסוימת. עוד נטען, שהנתבעות השתמשו ברשת מחשבים כדי לעקוב ולעדכן את הגירסה של "פגסוס" שהותקנה על גבי מכשיריהם של "הקורבנות" (כפי שכונו על-ידי הנתבעות בכתב התביעה). נטען, כי באמצעות רשת זו הנתבעות סיפקו שירותי תמיכה ושלטו על התפעול של לקוחותיהם ב"פגסוס". עוד נטען, כי הנתבעות מספקות תמיכה טכנית ללקוחותיה המשתמשים ב"פגסוס".

4. נטען בכתב התביעה, כי בין ינואר 2018 ומאי 2019, הנתבעות יצרו, וגרמו ליצירת, חשבונות ווטסאפ ופייסבוק שונים והסכימו לתנאי השירות של ווטסאפ. לפי הנתבעות השתמשו או גרמו להשתמש בחשבונות אלה לשלוח תוכנה זדונית למכשירי יעד במדינות שונות, כולל קפריסין, ישראל, ברזיל, אינדונזיה, שוודיה והולנד, במהלך אפריל ומאי 2019. נטען כי הנתבעות השתמשו ברשתים במדינות שונות, כולל בארצות הברית, על מנת להתחבר אל מכשירי היעד.

5. נטען, כי הנתבעות ביצעו "reverse engineering" לאפליקציה של וואטסאפ ופיתחו תוכנה שאפשרה להן לחקות פעילות לגיטימית של וואטסאפ על מנת להפיץ תוכנה זדונית למכשירי יעד.

6. נטען, כי בין התאריכים 29.4.2019 ועד ה- 10.5.2019 השתמשו הנתבעות בשרתי וואטסאפ, כדי להפיץ תוכנת ריגול לכ-1400 מכשירים ניידיים לצורך ביצוע מעקב אחר משתמשי וואטסאפ מסוימים, לרבות עורכי-דין, עיתונאים, פעילי זכויות אדם, מתנגדים פוליטיים, דיפלומטיים ובכירי ממשל זרים אחרים. נטען, כי היעדים היו משתמשי וואטסאפ ממדינות שונות, לרבות בחריין, איחוד האמירויות ומקסיקו.

7. **סמכות שיפוט**: בכתב התביעה נטען כי לבית המשפט הפדרלי של מחוז צפון קליפורניה סמכות לדון בתביעה, הן בשל עילות התביעה המבוססות על חקיקה פדרלית, הן נוכח ה"diversity" (כאשר לא כל הנתבעים הם מאותה מדינה בארה"ב), והן בשל התקיימותה של סמכות פרסונלית ביחס לנתבעות. הנימוקים לקניית סמכותו של בית המשפט מתייחסים, בין היתר, לסכום התביעה העולה על 75 אלף דולר כמו גם להסכמתן של הנתבעות לתנאי השירות של וואטסאפ, אשר כוללים תניית שיפוט מכוחה יכול בית המשפט דן לקנות סמכות. כמו כן צוין כי הנוק לתובעות נגרם בקליפורניה ולכן ביהמ"ש מהווה את הפורום הנאות.

8. **עילות התביעה**: התובעות טוענות לארבע טענות עיקריות, ביחס לעילות התביעה:

Commented [VS1]: פסקה 26

Commented [VS2]: התובעות הן שנוקטות במונח קורבנות. הוספתי את הסוגריים.

Commented [VS3]: פסקה 28

Commented [VS4]: פסקה 29

Commented [VS5]: פסקה 30

Commented [VS6]: פסקה 33

Commented [VS7]: פסקה 34

Commented [VS8]: פסקה 35

Commented [VS9]: פסקה 43

Commented [VS10]: פסקה 43

Commented [VS11]: בעיקר פסקאות 10-12

הפרת חוק המחשבים הפדרלי - התובעות טוענות כי הנתבעות הפרו את חוק המחשבים הפדרלי (California Computer Fraud and Abuse Act, 18 U.S.C. § 1030) בכך שבפעמים שונות בין ה-29 לאפריל 2019 ועד ה-10 למאי 2019, הנתבעות ניגשו, השתמשו או הביאו לשימוש בשרתי האיתות והממסר (signaling servers and relay servers) של התובעות ללא הרשאה, במטרה לפרוץ כ-1400 מכשירים. על-פי הנטען, הנתבעות ביצעו הונאה לצורך השגת מידע מהמכשירים הפרוצים, ב"מחשבים" ו"מחשבים מוגנים" כהגדרתם בחוק.

התובעות טוענות כי הונאה זו כללה הסכמה כוזבת לתנאי השימוש של וואטסאפ, שליחת פקודות לא מורשות למחשבי התובעות והסוואת הפקודות כתנועות רשת לגיטימיות, על מנת לקבל גישה למכשירי ללא ידיעתם או הסכמתם של המשתמשים.

כתב התביעה מפרט כי פעולות אלו גרמו הפסד לתובעות, אשר כולל גם את המשאבים שנדרשו לשם החקירה ותיקון ההונאה. לפיכך, מבוקש פיצוי בגין הפסדים ונזקים אלה.

הפרת ה-California Comprehensive Computer Data Access and Fraud Act - התובעות טוענות כי הנתבעות הפרו חוק זה, המהווה חלק מחוק העונשין של מדינת קליפורניה (California Penal Code § 502), בכך שניגשו ביוזעין וללא הרשאה למערכות ורשתות המחשבים של התובעות על מנת לתכנן ולהוציא לפועל הונאה ותחבולה וכן לקבל כסף, רכוש ונתונים שלא כדין. נטען, כי הנתבעות ביוזעין וללא הרשאה ובניגוד לדיון ערכו שימוש בשרתים, מערכות ורשתות מחשבים, לרבות כאלה המצויים בקליפורניה. כמו כן, הן ערכו שימוש כאמור גם במערכות המחשב ורשתות המחשבים של התובעות.

לפי כתב התביעה, פעולות הנתבעות גרמו לתובעות להפסדים ונזקים, ובהם השימוש במשאבים לשם חקירה ותיקון הפגיעה במערכות, פגיעה בשמן הטוב של התובעות וכן בטיב היחסים ביניהן לבין המשתמשים שלהן ומשתמשים פוטנציאליים, בסכום שיוכח במשפט. כתב התביעה מפרט כי בהתאם לחוק העונשין של קליפורניה, התובעים זכאים הן לפיצויים נזיקיים, שכר טרחת עורכי דין וסעד של צו מניעה, והן לפיצויים עונשיים.

הפרת חוזה - לפי כתב התביעה, כאשר הנתבעות ערכו שימוש בשירותי וואטסאפ, הנתבעות הסכימו לתנאי השימוש של וואטסאפ ומחוייבות להן. צוין, כי התובעות ביצעו מצידן את חובותיהן הנדרשות לפי תנאי השימוש. נטען כי הנתבעות הפרו את תנאי השימוש של וואטסאפ, ובכך פגעו בוואטסאפ, וממשיכות לפגוע בה. עוד צוין, כי כאשר הנתבעות הסכימו והתחייבו לפעול לפי תנאי וואטסאפ, גם הן וגם התובעות ידעו, או יכלו לחזות באופן סביר, כי ייגרם נזק כזה לתובעות כתוצאה מהפרת תנאי השימוש על-ידי הנתבעות. כתב התביעה מפרט כי פעולות אלו גרמו הפסד לתובעות, אשר כולל פגיעה בשמן הטוב של התובעות וכן בטיב היחסים ביניהן לבין המשתמשים שלהן ומשתמשים פוטנציאליים וגם את המשאבים שנדרשו לשם החקירה ותיקון של מעשיהן של הנתבעות. לפיכך, מבוקש פיצוי בגין הפסדים ונזקים אלו.

הסגת גבול במיטלטלין (trespass) - עוד צוין בכתב התביעה כי הנתבעות הפריעו לזכות החזקה של התובעות במערכות המחשבים הנדונות, בין היתר באמצעות כניסה ושימוש, בשרתי התובעות בכדי להעביר קוד זדוני לצורך פגיעה שלא כדין במכשירים של משתמשים, וכל זאת ללא הרשאה מצד התובעות והמשתמשים. כתב התביעה מפרט כי פעולות אלו גרמו הפסד לתובעות, אשר כולל פגיעה בשמן הטוב של התובעות וכן בטיב היחסים ביניהן לבין המשתמשים שלהן ומשתמשים פוטנציאליים וגם את המשאבים שנדרשו לשם החקירה ותיקון של מעשיהן של הנתבעות. לפיכך, מבוקש פיצוי בגין הפסדים ונזקים אלו.

#### 9. הסעדים המבוקשים בכתב התביעה הם, בעיקרם, כדלהלן:

פסק דין שייקבע כי הנתבעות הפרו את החוק הפדרלי, החוק של מדינת קליפורניה ואת תנאי החוזה עם וואטסאפ, וכן כי הנתבעות הסיגו גבול ברכושן של התובעות;

צו מניעה קבוע לפיו לא יהיו רשאיות הנתבעות, והפועלים מטעמן כגון עובדיהן, סוכנים שלהם וכיוצא בזה כל מי שפועל עמם - להירשם, להיכנס או להשתמש בשירותי התובעות ולקחת חלק בכל פעילות שיש בה כדי לשבש את פעילותן או להפר את תנאי השימוש שלהן; לקחת חלק בכל פעילות או לאפשר פעילות שיש בה כדי להפר את תנאי השימוש של וואטסאפ או פייסבוק;

**Commented [VS12]:** היים – כינתי זאת "שרתים" אבל ראה את מלוא ההקשר ואם זה מספק = מוגנים מהעולם שלך יותר..

Defendants knowingly and without permission used and caused to be used WhatsApp Signaling Servers and Relay Servers, including servers located in California, in violation of California Penal Code § 502(c)(3).

**פיצויים לתובעות** לרבות פיצויי השבה, פיצויים סטטוטוריים ופיצויים עונשיים, בסכומים אשר יוכחו במשפט (סכום הפיצויים המבוקש לא צוי).  
**החור הוצאותיהן של התובעות**, ובכלל כך שכר טרחת עורכי דינן.

ב. פרטים כלליים אודות הליך הליטיגציה בבית המשפט בקליפורניה עד כה:

10. הליך הליטיגציה שנוהל עד כה בבית המשפט בקליפורניה, מתמקד בעיקרו בטענות מקדמיות, בקשה להחליט גילוי ראיות ובקשות שונות שהוגשו על-ידי הצדדים, כגון בקשה לפסילת עורכי הדין של התובעות, בקשה להשתתף סנקציות על התובעות ועוד. נכון למועד כתיבת בקשה זו, בית המשפט בקליפורניה טרם הכריע בשתי בקשות עיקריות התלויות ועומדות בפניו: בקשה לדחייה על הסף אשר הוגשה על-ידי התובעות ביום 2.4.2020 ובקשה להחליט הליך גילוי הראיות עד לאחר החלטה סופית בדחייה על הסף, שהגישו התובעות בתאריך 16.6.2020. להלן נעמוד בקצרה אודות הליכים אלה.

**בקשה לדחייה על הסף:**

11. ביום 2.4.2020 הגישו התובעות בקשה לדחייה על הסף של כתב התביעה. בקשה זו מבוססת, בין היתר, על הנימוקים העיקריים הבאים:

- היעדר סמכות שיפוט לבית המשפט משום שלנתבעים קיימת "חסינות ריבון גזרת" ("Derivative foreign sovereign immunity"). ביחס לכך, התובעות טענו כי המעשים שנטען שבוצעו, ככל שבוצעו, לא בוצעו על-ידי, אלא על-ידי ממשלות ריבוניות זרות שהן הלקוחות שלהן; הטענה היא שמאחר ואין סמכות שיפוט, לפי הדין האמריקאי, לדון בתביעה כנגד מדינות זרות בשל המעשים האמורים (מאחר ולא מתקיימים חריגים לחסינות הריבון לפי החוק האמריקאי בנושא, ה-FSIA), כך גם אין סמכות לדון בתביעה דומה נגד התובעות, אשר, לפי הנטען פעלו בשליחותן של אותן המדינות, ולכן זכאיות לחסינות גם כן.
- היעדר סמכות שיפוט פרסונאלית כלפי התובעות – בהקשר זה, בין היתר, צוין כי מדובר בחברה ישראלית, המנהלת את עסקיה בישראל, ואיננה עורכת עסקים בקליפורניה;  
**לבקשה צורף תצהיר** מטעמו של מר שלו חוליו, מנכ"ל ובעלים משותף של חברת NSO. בתצהיר מתייחס, בין היתר, מר חוליו לנקודות הבאות:
- חברת NSO היא חברת טכנולוגיה המעצבת טכנולוגיה עבור ממשלות וסוכנויות ממשלתיות למטרות של בטחון לאומי ואכיפת חוק;
- התובעות מאוגדות בישראל ושם מצוי מקום העסקים העיקרי שלהן; התובעות אינן מקיימות עסקים בקליפורניה ואין להן משרדים או עובדים בקליפורניה, או במקום אחר בארצות הברית; התובעות לא ביצעו פעולות הרלבנטיות לכתב התביעה בקליפורניה ולא כיוונו כל מעשה הרלבנטי לכתב התביעה כלפי קליפורניה;
- **המכירות** של תוכנת "פגוס" כפופות לרגולציה של ממשלת ישראל. הייצוא של תוכנת "פגוס" מצוי תחת רגולציה של מערך הפיקוח על הייצוא **הבטחוני**.
- החוזים של חברת NSO דורשים ממשתמשי הקצה בתוכנת "פגוס" להצביע על כך שהם שייכים לממשלה או שהם סוכנות מורשית מטעמה לצורכי בטחון לאומי או אכיפת חוק ולספק מסמכים נוספים ככל הנדרש, לצורכי אישור של משרד **הבטחון**;
- **משרד** הבטחון דורש מחברת NSO לספק תעודה חתומה ממשתמשי הקצה של תוכנת "פגוס" שבה הם מצהירים שהתוכנה תשמש רק לצורך מניעה וחקירה של טרור ופעילות פלילית;
- חברת NSO משווקת את טכנולוגיית "פגוס" רק לממשלות ריבוניות וסוכנויות מורשות לבטחון לאומי ואכיפת חוק, ועושה כן רק לאחר קבלת רישיון יצוא ממשד הבטחון. חברת NSO איננה משווקת או מוכרת את תוכנת "פגוס" לשימוש של יישויות **פרטיות**, האשמות התובעות בעניין זה שיקריות;

**Commented [VS13]:** חיים – ניסינו לשלב נקודות עיקריות אבל אני מציעה שתעיין בתצהיר במלואו כי הוא חשוב ומרכזי כרקע עבורך. פרטתי יותר עבורך – אבל אני לא בטוחה אם צריך להיכנס לכל הפרטים במסגרת הבקשה שלנו.

**Commented [VS14]:** חיים ראה התייחסותו של שלו גם לחברת: q cyber

I am the CEO and a co-founder of Defendant NSO Group Technologies Limited ("NSO"). Defendant Q Cyber Technologies Limited ("Q Cyber" and, collectively with NSO, "Defendants") is NSO's sole director and majority shareholder.

**Commented [VS15]:** סעיף 3

**Commented [VS16]:** סעיף 4

**Commented [VS17]:** פסקה 5  
 Sales of NSO's Pegasus technology are strictly monitored and regulated by the Government of Israel. The export of NSO's Pegasus technology is regulated under Israel's Defense Export Control Law ("ECL"),

**Commented [VS18]:** לצורכי קיצור לא התייחתי לפסקה הבאה

To export its Pegasus technology, NSO is required to register with the Israeli Ministry of Defense ("MoD"). Under the ECL, the MoD is empowered to investigate NSO and its business, refuse or cancel NSO's registration, or deny NSO's license, taking into account several factors, including the intended use of NSO's Pegasus technology and the identity of NSO's customers. The MoD can and does ask NSO to provide documentation about its customers and prospective customers and the intended uses of NSO's Pegasus technology by NSO's customers and potential customers. The MoD requires this documentation from NSO for

each export of NSO's Pegasus technology

**Commented [VS19]:** פסקה 7  
 NSO's contracts require Pegasus end-user customers to demonstrate that they are a government or an authorized agency for national security and law enforcement purposes of a government and to provide any other necessary documentation for approval by the MoD.

**Commented [VS20]:** פסקה 8  
 The MoD requires the NSO provide it with signed certificates from the end-users of NSO's Pegasus technology in which the end-users declare that NSO's Pegasus technology will be used only for prevention and investigation of terrorism and criminal activity.

**Commented [VS21]:** פסקה 9  
 NSO markets and licenses its Pegasus technology exclusively to sovereign governments and authorized agencies for national security and law enforcement purposes of governments and does so only after receiving the necessary export control licenses from the MoD. NSO do...

• באוקטובר 2017, שני נציגים של חברת פייסבוק פנו לNSO וביקשו לרכוש זכות שלימוש ביכולות מסוימות של "פגסוס" – אותה תוכנה אליה מפנות התובעות בכתב התביעה.

Commented [VS22]: פסקה 10

• ל"פגסוס" יש אמצעי הגנה טכנולוגיים ("technical safeguards"). אחת ההגבלות הרלבנטיות לתיק זה, היא שתוכנת "פגסוס" לא ניתנת לשמוש כנגד מספר מכשיר סלולארי אמריקאי או כנגד מכשיר המצוי בגבולות הטריטוריאליים של ארצות הברית;

Commented [VS23]: פסקה 14 לתצהיר

• הנתבעות אינן מפעילות בעצמן את תוכנת "פגסוס". הלקוחות הריבוניים של החברה הם אלה שמפעילים בעצמם את התוכנה, על מנת לקדם את האינטרסים הריבוניים שלהם של מאבק בטרור ובפשיעה חמורה. התפקיד של הנתבעות מצומצם ליעוץ וסיפוק תמיכה טכנית לסייע ללקוחות בהקמה – ולא בהפעלה – של תוכנת "פגסוס";

Commented [VS24]: פסקה 15

• אין לי ידיעה על שימוש בהודעות וואטסאפ על-ידי לקוחות של החברה, לצורך התקנת "פגסוס" על מכשיר מסוים. אם מי מהלקוחות עשה כן, הרי שהדבר נעשה מטעמו, לצרכי קידום אינטרסים ריבוניים של מאבק בטרור ובפשיעה חמורה, וללא מעורבות של הנתבעות;

Commented [VS25]: פסקה 17

• הנתבעות אינן מבצעות מעקב כנגד אף אחד ואף אוסרות מבחינה חוזית על הלקוחות שלהן להשתמש בטכנולוגיה לכל מטרה שאיננה מאבק בטרור ובפשיעה חמורה. אם ממשלה כלשהי ניצלה לרעה את תוכנת "פגסוס" שלא במסגרת המטרות הנ"ל – הדבר אינו בידיעתן של הנתבעות. כאשר הנתבעות חושדות בשימוש לא נאות, השימוש ללקוח זה יושעה לצורך חקירה בנושא, וככל שהחקירה תגלה שאכן נעשה שימוש ממושך שכזה, היא תפסיק לספק את השירות ללקוח;

Commented [VS26]: פסקה 18

• הליך של גילוי ראיות הנוגע לשימוש של לקוחותיהן של הנתבעות, ידרוש מממשלות ריבוניות לגלות מידע רגיש הנוגע לביטחון הלאומי, מודיעין ומבצעים הנוגעים לאכיפת החוק;

12. ביום 23.4.2020 הגישו התובעות את התנגדותן לבקשה לדחייה על הסף. במסגרת זו, טענו התובעות כי יש לדחות את הבקשה, והתבססו, בין היתר, על טענות לפיהן הנתבעות אינן זכאיות לחסינות – נגזרת או אחרת. לטענתן, דוקטרינות החסינות הרלבנטיות בדין האמריקאי (תחת Foreign Sovereign Immunity Act - ה"FSIA") אינה חלות ביחס לחברות פרטיות, וכן דוקטרינות החסינות הנגזרת איננה חלה ביחס לנתבעות. בתאריך 30.4.2020 הגישו הנתבעות כתב תשובה התומך בבקשתם לדחייה על הסף.

13. בקשה זו עודנה תלויה ועומדת להחלטת בית המשפט בקליפורניה.

14. יצוין, כי ביום 24.6.2020 הגישו הנתבעות בקשה נוספת, המבקשת למחוק את בקשת התובעים לסעד המניעתי אשר נכלל בכתב תביעה (ראו סעיף 5 למעלה). זאת בשל היעדר זכות עמידה (Standing), בטענה כי התביעה מתייחסת לטענות ביחס למעשי עבר, ואין באפשרותן של התובעות לבקש צו מניעתי ספקולטיבי הצופה פני עתיד, המתייחס לנוקים שעלולים להיגרם להן בעתיד. גם בקשה זו עודנה תלויה ועומדת. התובעות התנגדו לבקשה זו ביום 8.7.2020.

#### הליך גילוי ראיות:

15. ביום 2.6.2020 נשלחה לנתבעות בקשה לגילוי מסמכים ראשונה מאת הנתבעות. לנתבעת הוקצבו, בהתאם לכללי הפרוצדורה, 30 ימים לשלוח לתובעות את המידע המבוקש, אלא אם כן היא מקבלת אורכה או מגישה בקשה לעיכוב הליך גילוי מסמכים.

16. בין היתר, הבקשה נוקבת בדרישה להמצאה של מסמכים ותכתובות הנוגעים לשימוש במוצר על-ידי צדדים שלישיים, כולל licensing agreements, חומרי שיווק ועוד; מידע על פיתוח ובדיקת התוכנה של הנתבעות; מידע על ה reverse engineering שנעשה ביחס לואטסאפ; מסמכים המתארים את כל המידע ואינפורמציה (data and information) שחברת NSO או הלקוחות שלה השיגו מהיעדים או מכשירי היעדים (from the Target

Commented [VS27]: חיים – תשומת לבכם שהמידע ביחס לכל הבקשות לגילוי מסמכים – איננו מופיע בתיק הפומבי של בית המשפט. המידע הגיע אלינו מהחברה והיא זו שהעבירה לעיוננו את הבקשות השונות – כולל בקשות לצדדים שלישיים. יחד עם זאת בקשר לבקשה לגילוי שמוענה לנתבעות – היא צורפה כנספח לבקשת הנתבעות להתליית הליך הגילוי לבית המשפט.

Commented [VS28]: מדינת ישראל ידעה על הגשת הבקשה רק בתאריך 8.6.2020

Commented [VS29]: חיים הערה של מרלין: תשומת לבך שהבקשה מציינת כך (ראה עמ' 3 למטה – סעיף 1 instructions). החשש הוא שלמעשה החובה למסור מסמכים היא מתגלגלת במהלך הליטיגציה ולא מוקפאת נכון למועד מסוים. צריך לקחת זאת בחשבון בניסוח הצו, שכן ייתכנו מסמכים נוספים שיידרשו בהמשך. ראה את הכלל הרלבנטי שמזכירות התובעות – סעיף 26 שמפנות אליו. לשיחה בעל-פה עם מרלין

Commented [VS30]: חיים – ברירת המחל המופיעה על גבי הבקשה שתואמת את הפרוצדורה היא 30 ימים. בפרקטיקה הצדדים דנים ביניהם על לוחות הזמנים וככל שלא מגיעים להבנות פונים לבית המשפט.

Users or the Target Devices); כל המסמכים והתקשורת המאפשרים זיהוי של כל הלקוחות של NSO אליהן מתייחס כתב התגובה מטעם הנתבעות לבקשה לדחייה על הסף; כל המסמכים ששימשו לשיווק, מכירה או קידום של התוכנה, לרבות מסמכים או תקשורת הקשורים לוואטסאפ או פייסבוק בכל צורה; גילוי מסמכים ותכתובות ביחס לזיהוי חולשות של וואטסאפ ופייסבוק, בתקופה שבין ינואר 2014 ועד דצמבר 2019.

17. עוד יצוין, כי הבקשה מתייחסת להגדרה רחבה למושג "מסמכים" (ראה סעיף 4 לחלק ההגדרות בבקשה לגילוי מסמכים) הכוללת גם התייחסות למסמכים, מידע, תוכנות מחשב, מידע המאוחסן אלקטרונית וכל דבר מוחשי אחר בהתאם לכלל 34 לכללי הפרוצדורה הפדרליים – שזו, כך להבנת המבקשת, הגדרה רחבה מאוד.

18. במקביל, החלו הנתבעות לפנות לצדדים שלישיים – חברות ואנשים פרטיים - הנמצאים בארצות הברית, עם צווי זימון להוצאת מסמכים או צו זימון למסירת עדות.

19. בתאריך 16.6.2020 הגישו הנתבעות בקשה להתליית הליך גילוי המסמכים וזאת עד להחלטה סופית בבקשתן לדחייה על הסף. יוער, כי בבקשתה זו ציינו הנתבעות את הפסקה הבאה ביחס למדינת ישראל:

"After a review of these requests, NSO has identified that they include requests for information that is either confidential or detrimental to the national security of the State of Israel. As such, NSO has notified the State of Israel of the discovery requests and is currently reviewing its legal obligations to protect such information from disclosure. The State of Israel is also considering its position with respect to the requests".

20. ביום 30.6.2020 התובעות הגישו התנגדות לבקשה להתליית הליך גילוי הראיות. בין היתר, הדגישו הנתבעות כי הטיעון לגבי "חסינות ריבון זר נגזרת" (שתחול לגבי חברות פרטיות) הוא טיעון חדשני (novel) שקבלתו תדרוש הרחבה לא מוצדקת של הלכות של בתי המשפט במחוז הפדרלי שאליו משתייכת קליפורניה. לטענתן, הנתבעות לא הציגו כל פסיקה התומכת בטיעון חדשני זה. עוד נטען, כי לא ניתן לבסס התליה של הליך גילוי הראיות בהתבסס על חסינות ריבון נגזרת פוטנציאלית, שכן טיעון זה, מעבר לחדשנותו כאמור, דורש כשלעצמו גילוי ראיות ביחס לטיב מעשיהן של הנתבעות ובאיזה מובן, אם בכלל, פעלו תחת הנחייתן של מדינות זרות. עוד טענו הנתבעות, בין יתר הטיעונים שהוצגו, כי הנתבעות העלו אך באופן ספקולטיבי את ההתנגדות האפשרית של מדינת ישראל או ממשלה זרה אחרת מטעמים של בטחון לאומי – דבר שאינו מצדיק התליה של כל הליך הראיות. נטען, כי כל התנגדות לגילוי ראיות תוכל לידון במסגרת הליך גילוי הראיות, ומדינת ישראל תוכל להתייצב בהליך לצורך כך, כפי שעשתה במקרים אחרים.

21. ביום 7.7.2020 הגישו הנתבעות את כתב התשובה בתמיכה לבקשתן להתליית הליך גילוי הראיות. הנתבעות מתייחסות, בין היתר, לטענה ביחס לחסינות ריבון נגזרת, כך שחסינות זו מגוננת מפני כל השתתפות בהליך הליטיגציה, ועל כן לא ניתן להמשיך בהליך גילוי הראיות כל עוד טענה זו תלויה ועומדת. עוד נטען, כי בית המשפט איננו זקוק להליך גילוי הראיות על מנת להכריע בבקשה לדחייה על הסף. כמו כן, נטען שדחייה לא תגרום נזק מהותי לתובעות. כמו כן הנתבעות מדגישות שוב כי הבקשה לגילוי מסמכים מהווה "מסע-דיג" לא ראוי ורחב, שיטיל נטל משמעותי על הנתבעות.

22. בקשה זו עודנה תלויה ועומדת להכרעת בית המשפט בקליפורניה.

**Commented [VS31]:** לחיים – פייסבוק כנראה עשו typo בבקשה שלהם – כי הם כתבו כך: • בקשה מס' 25: All Documents and Communications sufficient to identify all NSO Customers referenced in the Defendants' Opposition to the Motion to Dismiss;

היות וה-MTD הוגשה על-ידי הנתבעות, הרי שהן לא הגישו התנגדות לכך ופייסבוק עשו פה איזושהי טעות סופר. כנראה שהכוונה היתה להתנגדות שהגישו הנתבעות לבקשה.

**Commented [VS32]:** חיים – הוימונים אצלנו אם במקרה תצטרך. על פי הכללים התובעים חייבים למסור העתק של כל פנייה לצד ג' גם לנתבע.

**Commented [VS33]:** תוספת שלנו כדי להבהיר.

**Commented [VS34]:** התובעות מפנות להליך הבנק הסיני.

**Commented [VS35]:** חיים – לדיון בעל-פה כדאי שתשקול להתייחס לאופי הרחב של הליך גילוי הראיות המתבצע בארה"ב, כדי להסביר בין היתר את החשש של המדינה מהליך זה. בקשנו מעורכי הדין להציע איזושהו נוסח כללי שאפשר לומר בהקשר הזה. ראה נא (באנגלית):

In civil litigation in the United States, the US federal courts, in accordance with the US FRCP, allow for broad discovery of documents and information. Plaintiffs "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26(b)(1). Information "need not be admissible in evidence to be discoverable," *id.*, and "[d]istrict courts have broad discretion in determining whether evidence is relevant for discovery purposes," *Greer v. Elec. Arts, Inc.*, No. 10-cv-3601, 2012 WL 299671, at \*1 (N.D. Cal. Feb. 1, 2012). Potential sources for discovery include hard-copy documents, electronic documents, emails, WhatsApp/Signal/SMS messages, and other data. Therefore, it is not uncommon in large cases for courts to allow the production of hundreds of thousands or millions of documents. In addition, the US FRCP permit the parties to take the testimony of witnesses, under oath before a court reporter, as part of the discovery process. The rules authorize up to 10 depositions per side, but the parties may ask the court to authorize more. A party may seek and compel discovery from both other parties and non-parties to the litigation, and non-parties bear their own costs in responding to discovery requests.