

**בבית משפט השלום**  
**בראשון לציון**

**התובע:** קבוצת אן.אס.או. טכנולוגיות בע"מ, ח.פ. 514395409

מרח' גלגלי הפלדה 22, הרצליה  
ע"י עוה"ד משה מזור (מ.ר. 46901) ו/או גלעד רונן (מ.ר. 65897)  
גולדפרב זליגמן ושות', עורכי דין  
מרחוב יגאל אלון 98 (מגדל אמפא), תל אביב  
טל': 03-7101666; פקס': 03-6089843  
[gilad.ronen@goldfarb.com](mailto:gilad.ronen@goldfarb.com)

וכן ע"י עוה"ד רועי בלכר (מ.ר. 16312)  
ממשרד קריספין רובינשטיין בלכר ושות'  
מגדל בסר 4, רח' מצדה 7, בני ברק, 5126112  
טל': 03-3202021; פקס': 03-3202031

**-נגד-**

**הנתבעים:**

1. חטיבת כלכליסט – ידיעות אחרונות בע"מ, ח.פ. 510103922
  2. יואל אסתרן (אסתרן), ת.ז. 51286425
  3. גלית חמי (חמי), ת.ז. 23798101
- כולם מרח' נח מוזס 1, ראשון לציון 7565233

כולם ע"י עוה"ד ט. ליבליך, מ.ר. 15396 ו/או מיה כץ, מ.ר. 76812  
ממשרד עו"ד ליבליך-מוזר-גליק  
רח' נמל תל-אביב 40 (בית יואל) תל-אביב, 6100201  
טל': 03-5442370, פקס': 03-5442375  
[LM@lm-adv.co.il](mailto:LM@lm-adv.co.il)

המועד האחרון להגשת כתב הגנה: 8.5.22

המועד בו הומצא כתב התביעה: 27.2.22<sup>1</sup>

**כתב הגנה**

<sup>1</sup> תקנה 30 לתקנות סדר הדין האזרחי, התשע"ט-2018.

"NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent" (U.S. Department of Commerce, 3.11.2021). (מעלה ואילך ההדגשות אינן במקור, הח"מ)

### תמצית הטענות

1. **הנתבעים יטענו מיד בראשית כתב הגנה זה כי כל אשר פורסם – הוא אמת, אין בו לשון הרע, היה בו עניין ציבורי רב והוא נכתב בתום לב ובכל מקרה על הפרסום חלות ההגנות לפי חוק איסור לשון הרע, תשכ"א-1965 (להלן: "החוק"), לרבות, אך לא רק הגנת אמת דיברתי (ס' 14 לחוק) והבעת דעה בתום לב (ס' 15 לחוק).**
2. **מדובר בתביעה מופרכת, צינית ומסוכנת המוגשת תוך ניסיון להשתיק את הנתבעים בפרט ואת העיתונות החוקרת בכלל. בית המשפט הנכבד מתבקש שלא לאפשר זאת.**
3. **פעילותה האסורה והלא מפקחת של התובעת נחשפה בפני העולם, פעילות שממשלת ארצות הברית - לשכת התעשייה והביטחון של מחלקת הסחר בארה"ב (The commerce Department's Bureau of Industry and Security - BIS) קבעה כי בכך נכנסה ל'רשימה השחורה' של ישויות אשר ידועות בהתנהלותן הנוגדת את מדיניות הבטחון של ארצות הברית, וכי נאסר לקיים איתה קשרי מסחר:**

"The ERC determined that NSO Group and Candiru be added to the Entity List based on § 744.11(b) of the EAR: Entities for which there is reasonable cause to believe, based on specific and articulated facts, that the entity has been involved, is involved, or poses a significant risk of being or becoming involved in **activities that are contrary to the national security or foreign policy interests of the United States and those acting on behalf of such entities. Specifically, investigative information has shown that the Israeli companies NSO Group and Candiru developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers**"<sup>2</sup>.

4. **עוד הודיעה ממשלת ארצות הברית כי קיימות נגד התובעת די ראיות להוכחת מעורבותה בפיתוח ואספקה של תוכנות ריגול לממשלות זרות העושות בהן שימוש אסור ופוגעני לניטור ומעקב אחר אישי ציבור, עיתונאים, פעילי זכויות אדם, אקדמאים ועוד<sup>3</sup>.**
- כך לדוגמא, בעת האחרונה פורסם בעיתון 'The Guardian'<sup>4</sup>:

**"Spanish prime minister's phone 'targeted with Pegasus spyware"**

5. **נוכח האמור - מוטב היה לתובעת כי תרכין ראשה ותתרכז בעובדות המטרידות שמועלות נגדה ולא תפנה להליך משפטי בטענה כי נפגע שמה (הטוב!) כאשר ידוע גם לה כי אין לטענותיה כל בסיס, לא משפטי ולא עובדתי.**
6. **לא בכדי הודיעה התובעת בכתב תביעתה כי היא בוחרת שלא להתייחס לפרסומים הנוגעים לפעילות משטרת ישראל, שכן האמור בפרסומים אלו כבר איננו מוכחש - לא על ידי משטרת ישראל ולא על ידי**

<sup>2</sup><https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list>

<sup>3</sup><https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>

<sup>4</sup><https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware?source=techstories.org>

התובעת. אולם אין בכך בכדי להפחית מחומרת כזביה של התובעת בכל הנוגע להפעלת הרוגלה על ידי משטרת ישראל. **התובעת לא רק טענה כי המערכת אינה בשימוש בישראל, אלא הגדילה להצהיר "אין אפשרות לפגסוס לתקוף מספרים ישראלים"** (וראו ראיון מנכ"ל NSO, שלו חוליו בגלי צה"ל מיולי 2021) <sup>5</sup> **כעת ברור כי הצהרה זו, כמו רבות אחרות, היא שקרית מתחילתה ועד סופה.**

7. ובתמצית - התובעת לא רק סיפקה מוצר באמצעותו נעשו פעילויות לא מפקחות וכיום אף התברר שהן בלתי חוקיות במדינות שונות, אלא שהיום ברור כי התובעת הציגה מצגים סותרים ומטעים לגבי המערכת שלה ויכולותיה לנטר פעילות שבוצעה בה, והכל כפי שיובהר בכתב הגנה זה.

8. יתרה מכך, מלבד אמירות בעלמא נגד אמיתות הפרסום מושא כתב התביעה, התובעת לא מציגה ולו בדל ראיה או ביסוס עובדתי לטענותיה. כאשר מדובר בחברה שהציגה מצגים סותרים לגבי מערכותיה וטענה טענות שהוכחו כשקריות, **מן הראוי היה שלא תעלה טענות בעלמא אלא תצרך אסמכתאות כלשהן לנכונות טענותיה.**

9. אמיתות וחשיבות הפרסום מתחדדות גם נוכח קביעות שניתנו בעניינה של התובעת על ידי גורמים רשמיים ומדינתיים לפיהן: היא מקיימת קשרים עסקיים, בין היתר, עם גורמים לא מורשים ומדינות חשוכות; ראשיה נתפסו משקרים בהצהרתם כי תכנת הריגול "פגסוס" לא מופעלת על אזרחים ישראלים; נקבע, בין היתר, על ידי בית המשפט הגבוה לדיני משפחה בבריטניה (High Court of Justice, Family Division) כי שליט דובאי עשה שימוש לא חוקי ברוגלה של התובעת והפעילה נגד גרושתו במסגרת הליכי גירושין; כי האיחוד האירופי בוחן הטלת סנקציות עליה; כי שמה נקשר עם רצח העיתונאי הסעודי ג'מאל חאשוקג'י וכי מתנהלים נגדה הליכים שונים בבתי המשפט על ידי מי שנפגע ממוצריו ובני משפחותיהם. **מצ"ב פס"ד הבריטי ומסומן 1.**

10. בשל פעילותה אף הוגשו נגד התובעת תביעות על ידי חברות טכנולוגיות אחרות, ובכלל זה חברת מטא (פייסבוק בשמה הקודם) וחברת אפל בגין פריצות למכשירים על ידי רוגלת פגסוס באמצעות אפליקציות מטא ואפל, וכן על ידי אנשים פרטיים הטוענים כי נעשה שימוש בתכנת "פגסוס" נגדם.

11. **ברקע הדברים יש לציין כי התובעת נמצאת בהליכים לפי חוק חדלות פירעון ושיקום כלכלי, תשע"ח-2018 ומתמודדת עם סכסוכים פנימיים מכוערים בין בעלי המניות לבכירי החברה וכן מול משקיעיה.** משכך כבר עתה יש לבחון האם התובעת מוסמכת להגיש תביעה זו נוכח ההליכים המתנהלים נגדה.

12. שמה (הרע) של התובעת הוא תוצר של כל האמור ועוד. הפרסומים החשובים נשוא התביעה הם זרקור על פעילות שנחשפה זה מכבר על ידי גופים רשמיים, גופים עיתונאיים בארץ ובחו"ל (ביניהם הוויינגטון פוסט, גרדיאן, ניו יורק טיימס ועוד) וקביעות של בתי המשפט ברחבי העולם בנוגע לפעילותה הפוגענית – ועל כן, לא רק שאין התובעת יכולה להתהדר בשם טוב אלא שאין לתובעת אלא להלין על עצמה בכך שבחברה לפעול בניגוד לדין הישראלי והבינלאומי ובכך ששמה ללעג וסכנה את זכויות היסוד וחיייהם של רבים.

13. קיים אינטרס ציבורי עליון וחשוב בפרסומים אשר עד היום נמצאים במרכז השיח הציבורי, תקשורתי ומדיני כאחד, בארץ ובעולם. נדמה שאין חולק על כך, והקמת ועדות (בארץ ובעולם) לבדיקת חוקיות פעילות התובעת היא עוד ראיה לכך.

14. לאור כל האמור, הרי שהגשת תביעה זו בגין פרסומים שיש בהם בכדי להאיר על פעילות המחשכים של התובעת - מהווה "צעד נואש ואחרון" בניסיונה הכושל של התובעת להציל את עורה ואת שמה.

<sup>5</sup><https://glz.co.il/%D7%92%D7%9C%D7%A6/%D7%AA%D7%95%D7%9B%D7%A0%D7%99%D7%95%D7%AA/%D7%90%D7%99%D7%9C%D7%A0%D7%94-%D7%93%D7%99%D7%99%D7%9F/%D7%90%D7%99%D7%9C%D7%A0%D7%94-%D7%93%D7%99%D7%99%D7%9F22-07-2021-0801/%D7%9E%D7%A0%D7%9B%D7%9C-nso-%D7%91%D7%97%D7%A8%D7%A0%D7%95-%D7%A9%D7%9C%D7%90-%D7%9C%D7%A4%D7%A2%D7%95%D7%9C-%D7%A0%D7%92%D7%93-%D7%9E%D7%A1%D7%A4%D7%A8%D7%99%D7%9D-%D7%99%D7%A9%D7%A8%D7%90%D7%9C%D7%99%D7%9D-%D7%95%D7%90%D7%9E%D7%A8%D7%99%D7%A7%D7%A0%D7%99%D7%9D>

### פירוט העובדות הדרושות לעניין

15. כתב התביעה המסורבל שהגישה התובעת לא מאפשר להבין מה הם הפרסומים המקימים, לשיטתה, עילות תביעה בגין הוגש כתב התביעה נשוא הליך זה. על כן, יתייחסו הנתבעים לטענות המהותיות שעלו בכתב התביעה כדלקמן והם שומרים על זכותם לתקן את כתב הגנתם לכשיתוקנו הפגמים בכתב התביעה.

### **'מערכת פגסוס שואבת ללא הבחנה וללא סינון, ומבלי שנעשה ניזון על ידי התובעת'**

16. התובעת טוענת בכתב התביעה כי הפרסום מיום 2.2.22 לפיו מערכת פגסוס (להלן: "**פגסוס**" או "**הרוגלה**" או "**התוכנה**" לפי העניין והדבק) שנמכרה למשטרת ישראל איננה מנוונת - אינו נכון [ס' 21-22 לכתב התביעה]. במילים אחרות, טוענת התובעת - מערכת פגסוס שנמכרה למשטרת ישראל היא דווקא כן מנוונת (אלא שלגבי השימוש המדויק שנעשה על ידי משטרת ישראל בתוכנה התובעת מצהירה כי אין לה כוונה להתייחס)<sup>6</sup>.

17. דינה של טענה זו להידחות שכן הפרסום לעניין זה הוא **אמת**, כפי שאף נמסר מפי פרקליטות המדינה, ונסביר.

18. מערכת "פגסוס" מסוגלת לאסוף מידע מהמכשיר המודבק ב-3 רמות שונות:

19. **משיכת מידע ראשוני** (initial data extraction) – משיכה של מידע קיים על המכשיר. היינו, מידע שנוצר **קודם** למועד ההדבקה ויכול לכלול: היסטוריית הודעות, פרטי אנשי קשר, היסטוריית שיחות, מידע מלוח שנה, היסטוריית חיפושים ועוד. שימוש בפונקציית משיכת מידע ראשוני הוא אופציונלי ומחייב כי הרוגלה תימכר כך שאופציה זו תותקן ותהיה זמינה למפעיל. תכנה מנוונת היא, לדוגמא, תכנה שנמכרת ללא אופציה זו.

20. **ניטור פאסיבי** (passive monitoring) – מרגע שהמכשיר הודבק, הרוגלה מנטרת ואוספת כל מידע **חדש** שנצבר עליו בזמן אמת. כלומר, כל פעולה שנעשית במכשיר נאגרת ומתועדת, לרבות שיחות והודעות נכנסות ויוצאות, מיקום בזמן אמת ועוד.

21. **משיכה אקטיבית של מידע** (active collection) – בקשות ספציפיות של המפעיל לאיסוף מידע ספציפי. אופציה זו מאפשרת למפעיל, בין היתר, לבצע פעולות בזמן אמת במכשיר המודבק ולאסוף מידע ספציפי מהמכשיר ומסביבתו, כך למשל: ניטור שיחות, הקלטה של הסביבה באמצעות המיקרופון במכשיר, לקיחת תמונות, צילום מסך ועוד. אופציה זו מאפשרת למפעיל **לייצר** מידע שהוא מעוניין לאסוף, בשונה מתוכנות רוגלה אחרות שמבוססות על איסוף מידע שנוצר באופן טבעי.

22. כך, במסגרת הליך שמיעת הראיות בתיק הפלילי שהוגש נגד ראש הממשלה לשעבר בנימין נתניהו ובני הזוג אלוביץ' התגלה כי מכשירו הסלולרי של עד המדינה, פילבר, הודבק ברוגלת פגסוס. על פי הודעת גורם המשטרה **התכנה שאבה ממר פילבר מידע עודף מעבר למידע שהתבקש על ידי המשטרה**<sup>7</sup>. כמו כן, על פי הודעת הפרקליטות, המערכת ביצעה פעולות **בנוסף להאזנות סתר**, הכוללות גם **העתקה של אנשי קשר ופרטי מידע נוספים שהיו אגורים בטלפון**<sup>8</sup>. אמור מעתה: הרוגלה פעלה גם למשיכת מידע וגם לניטור פאסיבי.

- **מצ"ב תגובת המדינה בתיקי האלפים לפיה המערכת שאבה מידע שחרג מצו ביהמ"ש ומסומן 2.**

- **מצ"ב מסמך יחידת סיגינט במשטרה שנמסר מהפרקליטות ומסומן 3.**

<sup>6</sup> ראו לעניין זה, בין היתר, ס' 23 לכתב התביעה.

<sup>7</sup> וראו: <https://www.ynet.co.il/news/article/r1boda7jq>

<sup>8</sup> וראו: [https://www.mako.co.il/news-law/2022\\_q1/Article-999bfe33de20f71027.htm?Partner=interlink](https://www.mako.co.il/news-law/2022_q1/Article-999bfe33de20f71027.htm?Partner=interlink)

23. מהאמור לעיל עולה תמונה עובדתית ברורה – **תכנת פגסוס בה נעשה שימוש על ידי המשטרה פעלה ברמות שונות וללא מיקוד**. מעבר להאזנות סתר שהן ביטוי לניטור פאסיבי, התוכנה פעלה גם **למשיכת מידע** מהמכשיר שלא התבקש על ידי המפעילים ושלא נכלל בצו החיפוש שהתבקש (משיכת מידע ראשוני – שהיא כאמור אופציה שיש להתקין באופן מיוחד במערכת).

24. חשוב להבהיר – על מנת שרוגלה תוכל לפעול במכשיר הנדבק מבלי שבעלי המכשיר יוכל לשים לב לקיומה של הרוגלה במכשירו, הרוגלה חייבת לשבת על שכבת הפעלה בעלת גישה גבוהה. דרישה זו של הרוגלה היא שמקנה לה גישה לכלל המידע האצור במכשיר הנדבק וכן את היכולת לשתול נתונים ולשלוט על המכשיר המודבק עד כדי שליחת מסרונים ממנו, הוצאת שיחות, צילום תמונות ועוד. במילים פשוטות – הרובד בו מתמקמת הרוגלה במכשיר הנדבק הוא רובד בעל הרשאות גבוהות, רובד שמקנה לרוגלה גישה בלתי מובחנת לכל המידע במכשיר. על מנת למקד את הרוגלה לשליפה של מידע ספציפי על התובעת לנוון את האופציות שלמשטרה תינתן אליהן גישה. אלא שלדברי המשטרה (ביחס למידע שנשלף ממכשירו של מר פילבר) שלילת החומרים חרגה מהצו שניתן על ידי בית המשפט – משכך ברור איפוא כי המערכת שנמצאת בשימוש המשטרה אינה 'גרסה מנוונת'.

25. **משכך, טענת התובעת כי המוצר שנמכר למשטרה "מהווה גרסה מנוונת מאוד" היא שקרית ומטעה.**

**'תכנת פגסוס שנמכרה למשטרה מאפשרת מחיקה של רשומות' ("לוגים")**

26. "לשלמות התמונה יצוין כי **המערכת מאפשרת למשתמש לבצע תחזוקה הכוללת מחיקה של רשומות**", כך נכתב, שחור על גבי לבן, במסמך "ממצאי צוות הבדיקה בעניין האזנות סתר" מיום 21.2.22 (להלן: "**ועדת מררי**"). גם התובעת חוזרת על הדברים האמורים בכתב התביעה (סעי' 46), בזו הלשון: "וכי אמנם המשתמש יכול למחוק רשומות בממשק המשתמש של המערכת במסגרת פעולות תחזוקה...".

27. כמה עזות מצח נדרשת מהתובעת לטעון כי הפרסום מיום 10.2.22 (לפיו המערכת שנמכרה למשטרה מאופיינת ביכולת שלא לתעד, קרי- מחיקה, את הפעולות המבוצעות בה) איננו אמת שעה שוועדת מררי קבעה כי "המערכת מאפשרת למשתמש לבצע תחזוקה הכוללת **מחיקה של רשומות**" (ההדגשה אינה במקור, הח"מ, ר' נספח 9 לכתב התביעה).

28. ויצוין- אין נפקא מינא אם לתובעת יש גישה לרבדים עמוקים יותר במערכת בהם נשמר תיעוד הרשומות גם אם המפעיל מוחק אותן. הלוגים אליהם מכוונת התובעת נשמרים בבסיס נתונים פנימי אשר הגישה אליו נתונה לתובעת ולה בלבד, **והם אינם מהווים גורמי פיקוח ובקרה צייתיים על המפעיל**. לוגים אלו משמשים את התובעת לבקרה על השימוש שעושה המפעיל, לרבות השאלה האם הוא תואם את תנאי רישיון- קרי, למימוש אינטרסים כלכליים פנימיים שלה.

29. יתרה מכך, התובעת לא הציגה ולו בדל ראיה אשר יש בו בכדי להראות לבית המשפט הנכבד כי הלוגים הפנימיים 'שבשליטתה' ושאינן למשתמש אפשרות למחוק אותן – אכן אינם ניתנים למחיקה.

**'ללקוחות התובעת הוצעו מספר גרסאות לבחירה בכל הנוגע לתחזוקה וניהול הרשומות'**

30. בשים לב לשקריה של התובעת כפי שפורטו לעיל בכתב הגנה זה גם טענותיה כי "אין ומעולם לא הוצעו ללקוחות התובעת אפשרות לבחור גרסאות" של הרוגלה שמתוכננות כך שהלוגים לא יתועדו (וראו ס' 39 לכתב התביעה) – דינן להידחות. התובעת מודה כי במסגרת חוזי ההתקשרות שלה עם הלקוחות, האחרונים נדרשים להוסיף לרוגלה רכיב טכנולוגי המאפשר תיעוד ושיחזור של הפעולות. מכלל ההן הנך למד את הלאו: לרוגלה קיימת גרסה שלא מכילה את אותו רכיב טכנולוגי (עלום).

31. עוד יטענו הנתבעים כי העמימות הזועקת מכתב התביעה בכלל ובסעיפים ספציפיים בפרט מעידה על קלישות התביעה. כך, סעיף 35 לכתב התביעה כל כך עמום עד שאין אלא להסיק כי התובעת מנסה לגלות טפח ולכסות טפחיים ולהסתיר את האמת מהצדדים ומבית המשפט הנכבד. טענת התובעת כי הנתבעים 'לקו בפרשנות שגויה' אינה יכולה להוות עילת תביעה וודאי לא בנסיבות תביעה זו אשר התובעת מקפידה להסתיר את המפרט הטכנולוגי של הרוגלה.

32. ושוב, אין נפקא מינא אם בשכבה פנימית ומוצפנת של המערכת נותר תיעוד רשומות אליו אפשר להגיע רק באמצעות התובעת. למפעיל קיימת אפשרות לרכוש את המערכת כך שבשכבות העליונות של תחזוקה ואדמיניסטרציה, אלו שנמצאות בשליטתו וחשופות לביקורת וחקירה, לא יהיה תיעוד רשומות.

#### **'המערכת פועלת מענן מרוחק שנמצא בשליטת NSO'**

33. פסק הדין שניתן בבית המשפט הגבוה לדיני משפחה באנגליה ביום 5.5.2021 דן בטענה זו בהרחבה (נספח 1 לכתב ההגנה). עניינה של התביעה שהובאה בפני בית המשפט האמור הוא הליך גירושין בין שליט דובאי, לבין אשתו לשעבר, הנסיכה האיה מירדן, במסגרתו נטען כי **שליט דובאי עשה שימוש ברוגלת פגסוס על מנת לרגל אחרי אשתו והצוות המשפטי שלה**.

34. בפסק הדין נפסק כי **אכן נעשה אותו שימוש אסור ברוגלה**.

35. במסגרת פסק הדין נקבע עוד, כי הרוגלה עושה שימוש במרחב הווירטואלי על מנת ליצור מסלול סבך של נקודות עגינה בדמות שרתים מאובטחים (ענן) ובכך לטשטש את העקבות חזרה למפעיל. יש לציין כי התובעת עצמה מתהדרת ביכולותיה לאנונימיזציה שמטרתן, כאמור, למנוע את היכולת להתחקות אחר כתובת ה-IP של המפעיל.

36. על פי פסק הדין, המכשיר הנדבק העלה כי כתובות ה-IP בהן עבר המידע (נקודות העגינה) כללו גם כתובות שהיו רשומות על שם התובעת, ובמילים אחרות: לתובעת יש שליטה על כתובות ה-IP דרכן המידע עבר בדרך מהטלפון הנגוע למפעיל:

"He was then able to check back using historical internet scanning data to see which other IP addresses had returned the same response and found 83 addresses which were recorded as having done so between October 2013 and April 2014. **This included some IP addresses which were formally registered to NSO Group**" (פסקה 21 לפס"ד).

37. לא רק זאת, מחקר פורנזי ענק שפורסם בשנת 2021 שביצע ארגון זכויות האדם "אמנסטי" ביקש לבחון את העקבות הפורנזיות שנוצרו מאירוע הדבקה מכשירים בתכנת פגסוס.

38. ממצאי דוח הבדיקה של אמנסטי הצביעו כי **תכנת פגסוס עושה שימוש בשכבות רבות של שרתים בהם עובר המידע מרגע שליחת ההוראה על ידי המפעיל ועד רגע ההדבקה (והפוך לצורך שידור המידע שנאסף חזרה למפעיל)**. עוד נמצא כי קיימים מאות Domains הקשורים לתובעת שבהם נעשה שימוש בהרכבת מסלול האנונימיזציה.

39. עוד; לאחר השלמת המחקר, התבקש מכון המחקר "Citizen Lab" של אוניברסיטת טורנטו (ארגון הפועל לגילוי וחשיפה של פעילות התובעת מזה שנים רבות ואחראי לפרסומים רבים שהובילו לחקירות וחשיפות פעילותה הלא חוקית של התובעת) לוודא את מהימנות הליך הבדיקה של אמנסטי וממצאיה. סיטיון לאב ערכו בדיקה עצמאית (2021) ובחנו את שיטות המחקר של אמנסטי והגיעו למסקנה כי **המתודולוגיה של אמנסטי לגילוי הקשרים בין פעילות שנצפתה במכשירים הנבדקים (שהודבקו) בענן אמזון (Amazon CloudFront) לבין שרשרת השרתים בהם נעשה שימוש על ידי פגסוס היא מדויקת**.

40. לכך מתווספת העובדה כי בחודש יולי 2021 דווח כי שירותי האינטרנט של אמזון השביתו תשתית וחשבונות המקושרים ל-NSO.
41. נדמה איפוא כי גם לעניין זה מנסה התובעת בכל מאודה להטעות את בית המשפט בכתב התביעה על ידי שימוש בעמימות והסתייגויות.
42. וייאמר כבר עתה - אין בין העובדה שהמערכת מותקנת on premise אצל המפעיל לבין הטענה כי לתובעת יש שליטה על המידע באמצעות ענן מרוחק - דבר וחצי דבר.
43. כפי שנקבע כבר על ידי בית המשפט בבריטניה, וכפי שהובא במחקרים של אמנסטי וסיטיזן לאב (לגביהם לא הגישה התובעת תביעה למרות שפורסמו ברבים ויצרו הד ציבורי) – המידע שנאסף מהמכשיר המודבק עובר דרך מספר שרתים וכתובות IP על מנת לטשטש עקבות זיהוי של המפעיל.
44. עוד נמצא ונקבע בפסק הדין האמור כי חלק מכתובות ה IP והשרתים הם בבעלות/שליטה של התובעת ו/או נעשה בהם שימוש על ידי התובעת. על כן, הטענה לפיה המידע שעובר בין מכשיר היעד למפעיל נשמר כרשומה בענן שנמצא בבעלות התובעת – היא אמת, אין בה לשון הרע כלל וממילא נתמכת על ידי פרסומים רבים נוספים ואחרים שעליהם לא הלינה התובעת – ולא בכדי.
45. כמו כן, בימים האחרונים התפרסמה בניו יורקר כתבה של עיתונאי חתן פרס פוליצר רונן פארו במסגרתה הובאו דבריהם של עובדים ועובדים לשעבר בתובעת, אשר יש בהם כדי להוות עוד ראיה כי הפרסום נשוא התביעה הוא אמת:

"Employees told me that the company keeps its technology covert through an information-security department with several dozen experts. "There is a very large department in the company which is in charge of whitewashing, I would say, all connection, all network connection between the client back to NSO," a former employee said. **"They are purchasing servers, V.P.N. servers around the world. They have, like, this whole infrastructure set up so none of the communication can be traced."**

#### - הכתבה מצורפת ומסומנת 4.

46. עוד ביחס לעמימות שנוקטת התובעת נפנה לס' 41 לכתב התביעה: "התובעת אינה מפעילה את המערכות בעצמה והיא אינה חשופה למידע המבצעי שמופק באמצעות מוצריה". אלא שלא נטען כי התובעת היא זו שמפעילה, ולא נטען כי היא חשופה למידע המבצעי שהופק לבקשת המפעיל. אלא שהתובעת אינה מכחישה כי היא מחזיקה בשרתים וכתובות IP בהם עובר המידע מנקודת הקצה של המודבק לנקודת הקצה של המפעיל.
47. גם בס' 44 מנסה התובעת להתפתל בעמימות בניסוח: "התובעת אינה מפעילה את המערכות ואינה חשופה למידע; מערכות ה הלקוח נמצאות אך ורק באתר הלקוח..." – לכך נשיב: המערכות של הלקוח אכן נמצאות באתר הלקוח on premise אולם המידע עובר דרך עשרות אם לא מאות נקודות שמטרתן להסוות את זהות הלקוח. זהו כל הרעיון מאחורי מוצר התובעת. חלק מהנקודות מוחזקות על ידי התובעת. **ואת זה - התובעת לא מכחישה**. יתרה מכך - בדו"ח מררי צויין כי הבדיקה של צוות מררי נעשתה מול ממשק המשתמש ומול בסיס הנתונים הפנימי של המערכת, שהם שני מקומות אחסון ושליטה שונים. גם התובעת עצמה מסרה לצוות מררי כי היא בעלת גישה בלעדית למידע:
- "מהמידע שנמסר על ידי נציגי חברת NSO לנציגי צוות הבדיקה, השכבה של בסיס הנתונים הפנימי של המערכת אינה זמינה למשתמש, אלא יכולה להיות מוגשת על ידי החברה בלבד".

## הפרסום מיום 19.1.22 מהווה בין היתר גם הבעת דעה לגיטימית וסבירה ועל כן אין עילת תביעה נגד הנתבעים

48. הנתבעים יטענו כי מדובר במאמר דעה בסוגיה ציבורית מובהקת.
49. תחושותיה הסובייקטיביות של התובעת וחוסר שביעות רצונה מהדעה שהובעה במאמר אין בהן די על מנת לבסס עילת תביעה. כאמור, ברקע פרסום המאמר עמדה החלטת לשכת התעשייה והביטחון של מחלקת הסחר בארה"ב להכניס את התובעת ל"רשימה השחורה", נקבע כי מכרה את מוצריה גם לשליטים במדינות חשוכות אשר עשו בהם שימוש פרטי, פורסמו לגביה עשרות אם לא מאות מאמרי דעה בכל רחבי העולם ומתקיימים נגדה הליכים משפטיים בגין אחריותה הנזיקית לפריצה לא חוקית למטרות פוליטיות לטלפונים סלולארים של פעילי זכויות אדם ועיתונאים ובנוסף פסק הדין הבריטי אשר קבע מסמרות באשר לרוגלה ולשימוש הפסול שנעשה בה.
50. נוכח האמור, הדעה שהובעה בפרסום לפיה "פגסוס צריכה להימחק ויחד איתה גם NSO"; "מדובר בחברה רקובה מהיסוד"; "החברה איבדה כל אמינות" – מהווה הבעת דעה אשר נשענת על עובדות שאינן במחלוקת ואין היא חורגת מהסביר כמשמעות המונח בהלכה הפסוקה. הדברים האמורים נכונים גם ביחס לשאר חלקי הפרסום.
51. יתרה מכך, המאמר מבהיר לקורא על מה הוא מבוסס: (1) 'מייצרת מוצר מסוכן, כלי נשק, שאין לה שום יכולת לפקח על השימוש בו או להגביל אותו' – וראו כל שפורט לעיל, ובפרט השימוש בתכנה על מכשירו של פילבר וכן קביעת הרשויות האמריקאיות ביחס למוצרי התובעת ופסק הדין הבריטי (2) 'חברה שלא מהססת לשקר ושאי אפשר להאמין למילה אחת שמתפרסמת מפי הדוברים שלה' – וראו הרחבה להלן תחת הכותרת "אי קבלת תגובה" – ובנוסף נאמר מפורשות "המסקנה ברורה" – בכך מבהירים לקורא כי מדובר במסקנה של הכותב.

### טרוניית התובעת באשר לאי פנייה לתגובה:

52. בשיחות שקיימו הנתבעים עם דובר התובעת התגלו שקרים בוטים אשר מלמדים על חוסר מהימנות תגובותיה של התובעת.
53. דובר התובעת מסר באופן אישי לנתבעים כי רוגלת פגסוס לא הופעלה מעולם על מכשירים של אזרחים ישראליים. והנה - באופן מובהק ושלא ניתן להכחשה, כפי שגם נקבע בוועדת מררי, לא סתם נעשה שימוש על מכשירים של אזרחים ישראליים, אלא נעשה שימוש ממוסד על ידי המשטרה!
54. בנסיבות אלו, אין כל משמעות בפנייה לקבלת תגובה.
55. מטרת פנייה למושא כתבה לקבלת תגובתו היא לצורך בחינה מעמיקה של הטענות שיועלו על ידי המגיב ועל מנת לוודא שהפרסום עומד בפרמטרים העיתונאיים המקובלים. כאשר ברור כי מה שיימסר ממושא הכתבה הוא נעדר נאמנות ושקרי, כפי שכבר נוכחו לדעת הנתבעים בעבר, אין בתגובה סיבה שתצדיק בדיקות נוספות. מהימנותן המפוקפקת של הצהרות התובעת קיבלו משנה תוקף גם בשקרי של אחד ממייסדיה, ומי שהוא מנכ"ל התובעת - מר שלו חוליו, בראיון המוזכר לעיל. בראיון האמור מסר חוליו כי **חד משמעית** לא נעשה שימוש בתכנת פגסוס על מכשירים ניידים של אזרחים ישראלים, זאת כאשר, כידוע, המציאות העובדתית היא ההפוכה. גם מהאמור ניתן ללמוד כי בנסיבות העניין אין בהימנעות מקבלת תגובת התובעת משום חוסר סבירות כנטען על ידה.
56. ויודגש בית המשפט העליון כבר קבע שאי קבלת תגובה לא תשלול באופן אוטומטי את הגנת תום הלב, הכל לפי נסיבות המקרה.

הפרסומים מוגנים בין היתר גם על פי האמור בסעיפים 14 ו-15 לחוק איסור לשון הרע, תשכ"ה 1965

57. הנתבעים יטענו כי אין בפרסומים כל לשון הרע. עם זאת למעלה מן הצורך הנתבעים יטענו כי הפרסומים מוגנים על פי כל הגנות החוק החלות על פרסומים שכאלו.
58. מבלי לפגוע באמור לעיל, הנתבעים יטענו כי הפרסומים חוסים תחת סעי' 14 לחוק, באשר הם אמת והיה בהם עניין ציבורי חשוב ומובהק.
59. כמו כן, הפרסומים חוסים גם תחת הגנות תום-הלב הקבועות בסעי' 15 לחוק, ולרבות:
60. סעיף 15(2) לחוק – על הנתבעים חלה חובה חוקית מוסרית או חברתית להזהיר וליידע את הציבור מפני פעילותה של התובעת כפי שזו ידועה להם, ואשר לדעתם היא מבוססת בין היתר על פי קביעות של גורמים רשמיים מדינתיים, פעילות המשקפת התנהלות לא חוקית ומסוכנת לזכויות אדם בכל העולם.
61. סעיף 15(4) לחוק – דברי הנתבעים לא היוו לשון הרע ואולם למען הזהירות הם מהווים גם הבעת דעה על התנהגות התובעת בקשר לעניין ציבורי.
62. והכל, כאשר הנתבעים אמרו את הדברים בתום לב, ובאופן סביר ושאינו חורג מפרסומים שנעשו על התובעת בעבר.
63. לחלופין ולמצער, עומדות לנתבעים ההקלות מכוח סעיפים 19(2) לחוק איסור לשון הרע, שכן הנתבעים משוכנעים באמיתות כלל הפרטים.

#### **התייחסות לסעדים המבוקשים בכתב התביעה:**

64. אין לתובעת עילת תביעה נגד הנתבעים, והיא איננה זכאית לסעדים המפורטים, או לכל סעד אחר.
65. תביעה ללא הוכחת נזק אין פירושה קבלת פיצוי אוטומטי מבלי להוכיח ולו ראשית ראיה של נזק. התובעת איננה זכאית לפיצוי כלשהו, **וממילא לא הציגה ראיה לנזק שכביכול נגרם לה**. סעיף 7א לחוק המאפשר פיצוי סטטוטורי נועד לאפשר מתן סעד למי שאינו יכול להוכיח את שיעור נזקו, ולא נועד לפצות את מי שלא נגרם לו כל נזק. יתרה מכך, תביעה על סכום אסטרנומי של 1,000,000 ₪ וללא הוכחת נזק מלמד יותר מכל על התובעת ועל קלישות טענותיה.

#### **התייחסות פרטנית לסעיפי כתב התביעה כסדרם:**

66. מוכחש האמור בס' 1 לכתב התביעה מחוסר ידיעה.
67. לא מוכחש האמור בס' 2-4 לכתב התביעה.
68. מוכחש האמור בס' 5-9 לכתב התביעה.
- מבלי לגרוע מכלליות ההכחשה, ראו ס' 64-65 לכתב ההגנה.
69. מוכחש האמור בס' 10-11 לכתב התביעה.
- מבלי לגרוע מההכחשה, הפרסומים נשוא תביעה זו חוסים בין היתר גם תחת סעי' 14 לחוק, באשר הם אמת והיה בהם עניין ציבורי חשוב ומובהק ועל הנתבעים חלה חובה חוקית מוסרית או חברתית להזהיר וליידע את הציבור מפני פעילותה של התובעת כפי שזו ידועה להם, ואשר מבוססת על קביעות גורמים רשמיים מדינתיים, משקפת התנהלות לא חוקית ומסוכנת לזכויות אדם בכל העולם.
70. מוכחש האמור בס' 12 לכתב התביעה.
- מבלי לגרוע מההכחשה, החדרת הרוגלה למכשירים סלולריים של אזרחים ישראליים על ידי משטרת ישראל ושימוש בה באופן החורג מצווי בית המשפט שניתנו בעניין כבר פורסמה על ידי הפרקליטות והמשטרה – וזאת למרות ההכחשות השקריות של התובעת ושל הגורמים מטעמה. כמו כן, גם השימוש הבלתי מבוקר הוכח בעניינו של מר פילבר וראו הרחבה לעיל.
71. מוכחש האמור בס' 13 לכתב התביעה.

מבלי לגרוע מההכחשה, ראו סעי' 52-56 לכתב ההגנה.

**72. מוכחש האמור בס' 14-18 לכתב התביעה.**

מבלי לגרוע מההכחשה, ובשים לב לכל האמור בכתב הגנה זה הרי שלנתבעים עומדות כל ההגנות המצויות בחוק. האמור בפרסומים איננו קונספירטיבי או פרנואידי אלא, לצערנו ולצערם של תושבי העולם, הוכח על בשרם של אנשים פרטיים לאורך השנים האחרונות. מוצריה של התובעת הפכו לנחשקים במדינות 'בעייתיות' ועל ידי שליטים עריצים ואילו הדמוקרטיה ובראשן ארה"ב והאיחוד האירופי כבר הצהירו כי אין לתת יד לפעילותה של התובעת. גם ביחס לטענה כי מוצרי התובעת שימשו את רשויות האכיפה בישראל על מנת לרגל אחר אזרחים קיימות ראיות למכביר, ובראשן הודעות המשטרה ודוח הביניים של ועדת מררי.

מבלי לגרוע מההכחשה, הנתבעים פעלו בתום לב ובאופן סביר בנסיבות העניין ומכוח חובתם המוסרית והחברתית.

**73. לא מוכחשת סמכותו של בית המשפט הנכבד כפי שמפורטת בס' 19 לכתב התביעה.**

**74. מוכחש האמור בס' 20 לכתב התביעה** מחוסר רלוונטיות. מבלי לגרוע מההכחשה יצויין כי התובעת הצהירה מפורשות כי אין בכוונתה להתייחס לטענות שעלו ביחס לשימוש שעשתה משטרת ישראל ברוגלת פגסוס ולכן האמור בס' זה אינו רלוונטי למחלוקת בין הצדדים.

**75. מוכחש האמור בס' 21-23 לכתב התביעה.**

מבלי לגרוע מההכחשה, נפנה גם לס' 16-25 לכתב הגנה זה. בתמצית יצויין כי רוגלת פגסוס כפי שנמכרה למשטרת ישראל שואבת מהמכשירים המודבקים מידע באופן לא מובחן ומעבר למה שהתבקש ספציפית על ידי המפעיל. על בסיס האמור הרי שמדובר בגרסה לא מנוונת וכל שנאמר בפרסום הוא גם אמת.

**76. מוכחש האמור בס' 24-26 לכתב התביעה.**

מבלי לגרוע מההכחשה, הרי שהפרסום מיום 19.1.22 מוגן על פי האמור בס' 15 לחוק שכן הוא הבעת דעה לגיטימית וסבירה, וראו הרחבה לעיל תחת הכותרת "**הפרסום מיום 19.1.22 מהווה בין היתר הבעת דעה**".

**77. מוכחש האמור בס' 27-32 לכתב התביעה.**

מבלי לגרוע מההכחשה, הפרסום מיום 10.2.22 הוא אמת והתובעת לא צירפה ולו בדל ראיה שיעיד אחרת. כל כתב התביעה הוא גיבוב של טענות הנתבעות בעלמא. למרות שטענות התובעת בדבר אי פנייה לתגובה חוזרות על עצמן מספר פעמים ללא צורך, יפנו הנתבעים לס' 52-56 לכתב ההגנה.

**78. מוכחש האמור בס' 33 לכתב התביעה.**

מבלי לגרוע מההכחשה, הפרסומים נשוא תביעה זו נסמכים על ראיות שנאספו וקיבלו מעמד בכורה ברחבי העולם כפי שפורט בהרחבה בכתב הגנה זה. כל מה שנאמר בפרסום מיום 10.2.22 הוא אמת.

**79. מוכחש האמור בס' 34-38 לכתב התביעה.**

מבלי לגרוע מההכחשה יפנו הנתבעים לס' 26-29 לכתב ההגנה. בתמצית יצויין כי נקבע זה מכבר על ידי צוות ועדת מררי ביחס לרוגלת פגסוס כי "**המערכת מאפשרת למשתמש לבצע תחזוקה הכוללת מחיקה של רשומות**" ואין נפקא מינא אם לתובעת יש גישה מוצפנת לרבדים עמוקים בהם קיים תיעוד רשומות של מפעיל אין כל גישה אליו.

**80. מוכחש האמור בס' 39-40 לכתב התביעה.**

מבלי לגרוע מההכחשה יפנו הנתבעים לאמור בכתב ההגנה ובכל מקרה התובעת לא הכחישה כי ללקוחות שאינם משטרת ישראל - לא נמכרה, או למצער הוצעה, גרסה של הרוגלה שעוצבה כך שהלוגים לא ישמרו ולא יתועדו בשכבות שנגישות למפעיל. מכלל הלאו הנך למד את ההן.

81. מוכחש האמור בס' 44-41 לכתב התביעה.

מבלי לגרוע מההכחשה יפנו הנתבעים לס' 47-33 לכתב ההגנה. יצוין שוב, ובתמצית, כי נפסק על ידי בית המשפט בבריטניה שתוכנה שהושתלה במכשירה הסלולרי של גרושתו של שליט דובאי היא פגסוס שבבעלות התובעת וכי המידע שנאסף ונשלף ממכשירה הסלולרי עבר דרך כתובות IP שנמצאות בבעלותה של התובעת.

82. לא מוכחש האמור בס' 46-45 לכתב התביעה, ובמיוחד שרק בסיס הנתונים הפנימי של המערכת שנמכרה למשטרה נמצא בשרתים שהותקנו במשטרה (ואין בכך בכדי ללמד על כל שאר המיקומים בהם נמצא המידע שנשלף מהמכשיר הנגוע). כמו כן לא מוכחש כי המשתמש ברוגלת פגסוס יכול למחוק רשומות וכי לתובעת יש גישה מלאה לכל המידע שנאגר אצל המשתמש.

83. מוכחש האמור בס' 52-47 לכתב התביעה.

מבלי לגרוע מההכחשה, הנתבעים לא תיקנו דבר לאחר פרסום ממצאי ועדת מררי שכן הממצאים תומכים בפרסומים ובאמיתותיהם.

התמיהות שהעלו הנתבעים ביחס לממצאי הועדה שהופקו רק על בסיס נתונים שהועברו אליהם מהגופים החשודים (קרי, המשטרה והתובעת) הן הבעת דעה לגיטימית וסבירה בנסיבות העניין וכל ניסיון להשתיקה דינו להידחות.

84. מוכחש האמור בס' 58-53 לכתב התביעה וכל האמור בסעיפים אלו הוא חזרה על טענות שכבר עלו קודם לכן וניתנה להם התייחסות בכתב ההגנה. כמו כן, טענותיה של התובעת בס' 56-54 לכתב התביעה הן מבזות את הטוען להן וממילא אינן מצביעות על עילת תביעה ודינן להימחק מכתב התביעה. התובעת לא הביאה ולו בדל ראיה כי ההשמצות המופנות כלפי הנתבעים בסעיפים אלו הם אמת ונדמה כי כל מטרתן היא להשחיר את שמם של הנתבעים על ידי שימוש ציני בהליך משפטי.

85. מוכחש האמור בס' 60-58 לכתב התביעה (תשומת הלב שס' 58 חוזר על עצמו פעמיים).

לא מוכחשות מילות החוק כפי שהובאו בס' 59-58 אך מוכחשת רלוונטיות הסעיפים לעניין תביעה זו ובכל מקרה עומדות לנתבעים הגנות החוק לפי ס' 15-14 לחוק.

מבלי לגרוע מההכחשה, הפרסום בדבר מאפייניה הטכנולוגיים של התובעת הוא אמת והתובעת לא הביאה בכתב תביעתה בדל ראיה שיש בה בכדי לסתור טענה זו.

מבלי לגרוע מההכחשה, אי חוקיות פעילותה של התובעת כבר נקבעה על ידי הרשויות האמריקאיות כמפורט לעיל. כאמור, נקבע כי התובעת מספקת מוצרים באמצעותן מבוצעות עבירות על ידי מדינות "בעייתיות".

מבלי לגרוע מההכחשה, הפרסום מיום 19.1.22 הוא מאמר דעה וכל האמור בו מוגן תחת ס' 15 לחוק כאמור לעיל.

86. מוכחש האמור בס' 63-61 לכתב התביעה.

לא מוכחשות מילות החוק כפי שהובאו בסעיפים אלו, אולם מוכחשת הרלוונטיות שלהם לנתבעים. לנתבעים אין כל חבות לפי החוק בגין הפרסומים נשוא התביעה והם אינם לשון הרע, ובכל מקרה עומדות להם הגנות החוק כפי שפורט בהרחבה בכתב הגנה זה.

87. מוכחש האמור בס' 70-64 לכתב התביעה.

מבלי לגרוע מההכחשה, לעניין ההגנות שקמות לנתבעים, יפנו הנתבעים לס' 63-57 לכתב ההגנה; לעניין הטענה כי הנתבעים לא פנו לקבלת תגובה, יפנו הנתבעים לס' 56-52 לכתב ההגנה.

88. מוכחש האמור בס' 71-73 לכתב התביעה.

מבלי לגרוע מההכחשה, טענת התובעת כי פנייתה לא טופלה מכיוון שלא הוטמעו התיקונים שנדרשו על ידה- דינה להידחות. הנתבעים והתקנון המוזכר לא מחוייבים לתקן באופן אוטומטי פרסומים וודאי לא פרסומים שהם אמת והבעת דיעה לגיטימית. כמו כן, וכפי שפורט בהרחבה בכתב הגנה זה, ממצאי ועדת מררי דווקא תומכים בפרסומים ומעידים על שקריות של התובעת.

89. מוכחש האמור בס' 74-79 לכתב התביעה.

מבלי לגרוע מההכחשה, יפנו הנתבעים לס' 64-65 לכתב ההגנה. ביחס לסעד המבוקש (לראשונה) בס' 79 לכתב התביעה **לפרסום התנצלות** יובהר כי לבית המשפט הנכבד אין סמכות עניינית לחייב את הנתבעים בפרסום התנצלות כלפי התובעת, או לחייבם להפיץ את אותה התנצלות. סעד של פרסום התנצלות אינו קיים בחוק, ועל פי הפסיקה העקבית אין לבית המשפט הנכבד סמכות עניינית להעניקו לתובעת.

  
מיה כץ, עו"ד

ב"כ הנתבעים

  
ט. ליבליך, עו"ד

## נספחים - תוכן עניינים

מס'	שם הנספח	עמ'
1	פסק דין של בית המשפט הגבוה לענייני משפחה בבריטניה	13
2	תגובת המדינה בתיקי האלפים לפיה הרוגלה שאבה מידע שחרג מצו ביהמ"ש	54
3	מסמך מיחידת הסיגינט במשטרה	61
4	פרסום בניו יורקר של רונן פארו	63

## **נספח 1**

**פסק דין של בית המשפט  
הגבוה לענייני משפחה  
בבריטניה**

**עמ' 13**



Neutral Citation Number: [2021] EWHC 1162 (Fam)

Case No: FD19P00246, FD19P00380  
FD19F05020 and FD19F00064

**IN THE HIGH COURT OF JUSTICE**  
**FAMILY DIVISION**

Royal Courts of Justice  
Strand, London, WC2A 2LL

Date: 05/05/2021

**Before :**

**The President of the Family Division**

-----  
**Re Al M (Fact-finding)**  
-----  
-----

**Mr Charles Geekie QC, Mr Timothy Otty QC, Ms Sharon Segal, and Mr Daniel Burgess**  
**(instructed by Payne Hicks Beach) for the mother**  
**Lord Pannick QC, Mr Richard Spearman QC, Mr Nigel Dyer QC, Mr Andrew Green**  
**QC, Mr Godwin Busuttil, Mr Daniel Bentham, Mr Stephen Jarman and Mr Jason Pobjoy**  
**(instructed by Harbottle & Lewis) for the father**  
**Ms Deirdre Fottrell QC and Mr Tom Wilson (instructed by Cafcass legal) for the Children's**  
**Guardian**

Hearing dates: 13<sup>th</sup>, 15<sup>th</sup>, 16<sup>th</sup> & 19<sup>th</sup> April 2021  
-----

**Approved Judgment**

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

\*\*\*\*\*  
**THE PRESIDENT OF THE FAMILY DIVISION**

This judgment shall not be disclosed or circulated to anybody other than the parties and their legal advisers other than with the express permission of the Court



**Sir Andrew McFarlane P :**

**Introduction**

1. The focus of this judgment is the determination of a number of factual allegations that have been made in the course of ongoing proceedings relating to the welfare of two children. The children are Sheikha Al Jalila bint Mohammed bin Rashid Al Maktoum and Sheikh Zayed bin Mohammed bin Rashid Al Maktoum, who are now aged 13 and 9 years respectively. Their mother is Her Royal Highness Princess Haya bint Al Hussein. Their father is His Highness Mohammed bin Rashid Al Maktoum. The ultimate purpose of the proceedings is the resolution of issues relating to the children's welfare, in particular with respect to the contact that they are to have with their father and with respect to their education.
2. In 2019 the court conducted an extensive fact-finding process. In the 'First Fact-finding Judgment' handed down on 11 December 2019 ([2019] EWHC 3415 (Fam)) a number of very serious findings were made against the father. It had been anticipated by the court and the parties that no further fact-finding process would be needed and the court could, therefore, move on to determine the outstanding welfare issues. However, events in July and August 2020 have generated a number of additional factual allegations made by the mother against the father and those acting on his behalf in Dubai. As will become apparent, it has been necessary for the court to determine a number of legal and evidential issues between the parties relating to these new factual allegations before, finally, conducting a hearing to determine whether or not any of them is established.
3. In this judgment, following a recital of the detailed factual allegations that have been made, I will describe the legal context within which the factual matters fall to be determined and the various procedural steps that have been undertaken in preparation for the final hearing, before turning to the detailed evidence and, finally, to the court's conclusions.

**Factual allegations**

4. The mother seeks the following findings:
  - i. The mobile phones of the mother, two of her solicitors (Baroness Shackleton and Nicholas Manners), her Personal Assistant and two members of her security staff have been the subject of unlawful surveillance during the course of the present proceedings and at a time of significant events in those proceedings.
  - ii. The surveillance has been carried out by using software licensed to the Emirate of Dubai or the UAE by the NSO Group.
  - iii. The surveillance has been carried out by servants or agents of the father, the Emirate of Dubai or the UAE.
  - iv. The software used for this surveillance included the capacity to track the target's location, the reading of SMS and email messages and other messaging apps, listening to telephone calls and accessing the target's contact lists, passwords, calendars and photographs. It would also allow recording of live activity and taking of screenshots and pictures.

- v. The surveillance has occurred with the express or implied authority of the father.
5. At issue, are two basic assertions, firstly, whether any phones of those identified in paragraph 4(i) have been, in lay terms, hacked and, secondly, if the fact of hacking is established, whether it has been carried out by servants or agents of the father, the Emirate of Dubai or the UAE and whether the hacking has occurred with the express or implied authority of the father.

### The legal context

6. The legal context within which factual allegations are determined is well settled and is not controversial as between the parties. The burden of proof is on the party who makes the allegations, the mother in this case, and it applies both to the fact of hacking and the question of the attribution of responsibility. The standard of proof is the simple balance of probabilities. The burden of proof is not reversible and there is no responsibility on the father in this case to prove anything. In particular, if the court is satisfied that the fact of hacking is proved, that state of affairs does not establish a 'pseudo-burden' upon the father to prove that responsibility should be attributed to some other person or State (to adopt the phrase used by Mostyn J in *Lancashire v R* [2013] EWHC 3064 (Fam)).
7. Findings of fact must be based on evidence rather than speculation. In *Re A (Fact-finding: Disputed Findings)* [2011] 1 FLR 1817, Munby LJ (as he then was) said:

“(it is an) elementary proposition that findings of fact must be based on evidence, (including inferences that can properly be drawn from evidence) and not on suspicion or speculation.”

In *Re B (Care Proceedings: Standard of Proof)* [2008] UKHL 35 Baroness Hale (at paragraph 31) said:

“In this country we do not require documentary proof. We rely heavily on oral evidence, especially from those who were present when the alleged events took place. Day after day, up and down the country, on issues large and small, judges are making up their minds whom to believe. They are guided by many things, including the inherent probabilities, any contemporaneous documentation or records, any circumstantial evidence tending to support one account rather than the other, and their overall impression of the characters and motivations of the witnesses. The task is a difficult one. It must be performed without prejudice and preconceived ideas. But it is the task which we are paid to perform to the best of our ability.”

8. The court must consider all of the evidence, and consider the picture created by the evidential jigsaw as a whole. In *Re T* [2004] 2 FLR 838 Dame Elizabeth Butler-Sloss P described the process in these terms:

“...evidence cannot be evaluated and assessed separately in separate compartments. A judge in these difficult cases has to have regard to the relevance of each piece of evidence to other evidence and to exercise an overview of the totality of the

evidence in order to come to the conclusion whether the case put forward...has been made out to the appropriate standard of proof.”

9. The present case involves a good deal of expert evidence. It is for the court to determine the factual issues upon which expert opinion may then be offered. The role of the expert and of the judge are distinctly different as described by Ward LJ in *Re B (Care: Expert Witnesses)* [1996] 1 FLR 667:

“The expert advises but the judge decides. The judge decides on the evidence. If there is nothing before the court, no facts or no circumstances shown to the court which throw doubt on the expert evidence, then, if that is all with which the court is left, the court must accept it. There is, however, no rule that the judge suspends judicial belief simply because the evidence is given by an expert.”

10. Where more than one person or agency may be responsible for behaviour which the court has found proved, the court must be careful to ensure that a positive finding is only made against one or other on the balance of probabilities. The approach was correctly described by Lord Justice Peter Jackson in *Re B (A Child)* [2018] EWCA Civ 2127:

“20. Even where there are only two possible perpetrators, there will be cases where a judge remains genuinely uncertain at the end of a fact-finding hearing and cannot identify the person responsible on the balance of probabilities. The court should not strain to identify a perpetrator in such circumstances: *Re D (Care Proceedings: Preliminary Hearing)* [2009] EWCA Civ 472 at [12].

21. In what Mr Geekie described as a simple binary case like the present one, the identification of one person as the perpetrator on the balance of probabilities carries the logical corollary that the second person must be excluded. However, the correct legal approach is to survey the evidence as a whole as it relates to each individual in order to arrive at a conclusion about whether the allegation has been made out in relation to one or other on a balance of probability. Evidentially, this will involve considering the individuals separately and together, and no doubt comparing the probabilities in respect of each of them. However, in the end the court must still ask itself the right question, which is not who is the more likely, but does the evidence establish that this individual probably caused this injury? In a case where there are more than two possible perpetrators, there are clear dangers in identifying an individual simply because they are the likeliest candidate, as this could lead to an identification on evidence that fell short of a probability. Although the danger does not arise in this form where there are only two possible perpetrators, the correct question is the same, if only to avoid the risk of an

incorrect identification being made by a linear process of exclusion.”

11. The father’s case includes the suggestion that there may be a ‘pool of possible perpetrators’, if the fact of phone hacking itself is established. In *North Yorkshire County Council v SA* [2003] EWCA Civ 839, the Court of Appeal established that a person would only be included in the pool of possible perpetrators if the evidence established that there was ‘a likelihood or real possibility’ that they were the perpetrator. That approach was endorsed by the Supreme Court in *Re S-B (Children)* [2009] UKSC 17 where Baroness Hale said (paragraph 43) ‘if the evidence is not such as to establish responsibility on the balance of probabilities it should nevertheless be such as to establish whether there is a real possibility that a particular person was involved.’

### Foreign Act of State

12. As part of his response to the allegations, the father asserted in September 2020 that the ‘Foreign Act of State’ doctrine [‘FAS’] precluded the court from investigating the allegations. After a full hearing the court (The President and Mr Justice Chamberlain) held, in a judgment handed down on 20 October 2020 ([2020] EWHC 2883 (Fam)), that the FAS doctrine did not prevent the court from carrying out a fact-finding investigation and adjudicating upon all of the mother’s allegations. On 8 February 2021 the father’s appeal against this decision was dismissed by the Court of Appeal (The Master of the Rolls, Moylan and Andrews LJ; [2021] EWCA Civ 129). On 8 March 2021, the father’s application for permission to appeal was refused by the Supreme Court. Thus, it was only after that date the court was able to proceed with the fact-finding hearing.

### The origin of the mother’s allegations

13. In order to maintain the overall fairness of the court process it has been necessary to adopt certain novel, or at least out of the ordinary, procedural measures. Resort to these additional procedural steps were necessary largely in consequence of the two separate channels through which the mother’s principal solicitor, Baroness Shackleton, came to learn of possible phone hacking in the course of 5 August 2020.
14. The first contact to Baroness Shackleton was via a message from another solicitor, Mr Martyn Day of Leigh Day Solicitors, which informed Baroness Shackleton of the identity and role of a computer surveillance expert, Dr Marczak. The second, and entirely separate, source of information came in a telephone call from Mrs Cherie Blair QC who had been invited to make contact with Baroness Shackleton by a senior official in NSO Group, an Israeli based software company responsible for marketing highly sophisticated surveillance programs for the exclusive use of State Governments and their intelligence services [‘NSO’ or ‘NSO Group’].

(a) *Dr Marczak*

15. Dr William Marczak is a post-doctoral researcher in computer science at the University of California, Berkeley. He is also a research fellow attached to ‘Citizen Lab’, which is an independent research body based in Canada with an interest in electronic surveillance.

16. Through Citizen Lab, and independently, Dr Marczak has for some years conducted research into nation-state use of spyware and hacking tools to carry out covert surveillance against journalists, dissidents and other individual targets. It will be necessary to describe Dr Marczak's methods and his evidence in more detail at a later stage. For the present a broad overview will suffice.
17. To the ordinary layman phrases such as 'spyware' or 'malware' are likely to indicate the unwelcome deposit into their computer or mobile phone of a malevolent program which then seeks to extract confidential data or otherwise function in a destabilising manner. The software program which is at the centre of this fact-finding hearing, and which is manufactured and sold by NSO Group, operates in a different manner. The software is called 'Pegasus'. A principal feature of the Pegasus operation is that at no stage during the process of surveillance should it be possible to detect any trace of its covert processes. Thus, rather than requiring the owner of the device to be tricked into clicking on a link and downloading a subversive program onto their device, where it could then be detected by conventional antivirus software, the Pegasus software operates by linking the device with a remote server or servers, which may be anywhere in the world. The server will then send 'command and control' messages to the hacked device. Each of the remote servers used by Pegasus, and there are many, must, in common with any other internet connected device, have its own individual IP address ('IP' stands for 'internet protocol'). In order to cover up the trail of transmission of messages using Pegasus to and from a hacked device, command and control signals sent down the line will be likely to pass through a number of such 'proxy servers' before connecting to the ultimate controller, being an operative in the intelligence services of a particular customer State.
18. The trigger event that may cause a target device to communicate with a Pegasus proxy server may be a single click by the device's owner to a link in a spoof text message. Alternatively connection may be made without any action on the part of the device's owner at all by an 'over-the-air' method of infection, which involves sending a 'push message' that triggers the device to connect to the proxy server.
19. It follows that it is unlikely to be possible to detect that a phone or computer has been hacked by Pegasus software if the method of investigation is limited to searching for the electronic presence of spyware or malware even with the most sophisticated and professional antivirus search mechanisms. There will simply be no trace of Pegasus on the device because it does not need to maintain a presence there even for a very short time in order to control the device's functions and harvest data from it.
20. In order to detect the deployment of Pegasus software Dr Marczak has therefore had to adopt different methods of investigation. In broad terms these have involved the following three avenues:
  - (a) Identifying Pegasus proxy server IP addresses;
  - (b) Identifying unconventional applications ('apps') used by Pegasus;
  - (c) Spotting idiosyncratic grammar and syntax used by Pegasus software programmers.

21. A breakthrough occurred some few years ago when Mr Ahmed Mansoor, a human rights campaigner active in the Middle East, received a text message which seemed suspicious. Mr Mansoor passed his phone to Dr Marczak. Dr Marczak, having established the ability to monitor the phone's activity, clicked on the link and was able to detect and record the various IP addresses with which the device then fell into communication. Dr Marczak advised the court that the format of a spyware program's 'check-in' and a server's response to it is often unique to the particular family of spyware being used. Dr Marczak has the ability to screen computer messages across every single IP address in the world. He undertook this process with the check-in message generated by clicking on the link contained in the text message received by Mr Mansoor's phone. Dr Marczak was then able to record those IP addresses which returned a response consistent with the functioning of that seen on Mr Mansoor's phone. On that occasion he identified some 237 IP addresses in this way. He was then able to check back using historical internet scanning data to see which other IP addresses had returned the same response and he found 83 addresses which were recorded as having done so between October 2013 and April 2014. These included some IP addresses which were formally registered to NSO Group.
22. Dr Marczak labelled the historic list of sites 'version 1' and the sites found on the scan contemporaneously with the hacking of Mr Mansoor's phone as 'version 2'. He then used a period of months, or it may have been longer, to continue tracking the 237 IP addresses (version 2) found at the time that Mr Mansoor's phone was infiltrated. Whilst, no doubt to maintain maximum covert agility, many of these IP addresses are used only for a very short time, Dr Marczak noted that 3 of the 237 addresses came back into use at a later date with a new decoy trigger. By tracking this new decoy trigger in the same way and screening it across every IP address currently in use, he identified a further 1,091 IP addresses which he labelled 'version 3'.
23. Finally, and in a wholly different way, Dr Marczak has identified a particular idiosyncrasy of the Pegasus spyware based on the method used to forward data to subsequent servers. Dr Marczak labelled an earlier idiosyncrasy as the 'first fingerprint'. He has disclosed the detail of the first fingerprint and it forms part of the general process of detection that I have already described and which is already publicly available in articles and other papers that Dr Marczak has authored over recent years. Dr Marczak does not, however, understand that the further idiosyncrasy that he has spotted, and which forms his 'second fingerprint', is known to others and, particularly, not known to the NSO Group. It therefore has continuing investigative, and no doubt commercial, value to Dr Marczak and he has declined to disclose it openly in these proceedings.
24. Dr Marczak has also asserted the need for maintaining confidentiality over the identity of an individual, 'Mr X', whose telephone was, he asserts, hacked in the same time period as the alleged hacking of the phones of the mother, her solicitors and staff. I will turn in more detail to consider the evidence relating to Mr X's phone at a later stage. The purpose of referring to him now is to explain his relevance with respect to the decisions made relating to the overall fairness of the proceedings which have, indeed, been conducted on the basis that his identity has remained confidential as to the parties and the court.
25. Dr Marczak describes Mr X as 'a UAE activist'. In the summer of 2020 Dr Marczak was engaged in monitoring the internet traffic for several devices used by Mr X because

he suspected that Mr X might be targeted with spyware. Dr Marczak asserts that Mr X was previously targeted with Pegasus spyware in 2015 by the same State operator who targeted Mr Mansoor the following year. On 12 July 2020 and on 3 August 2020 Dr Marczak saw Mr X's iPhones download a substantial amount of encrypted data from servers pointed to by two domain names that he had identified as belonging to the version 4 group of NSO servers. In accordance with his usual practice Dr Marczak then followed up the lines of communication and sought to identify the IP addresses and other distinctive features of the attempted infiltration of Mr X's device. Once he had done so he then attempted to discover the identities of other victims that were communicating with these suspected Pegasus command and control proxy servers at the same time. This led Dr Marczak to spot the IP address of the firm of solicitors instructed in these proceedings by the mother, led by Baroness Shackleton, Payne Hicks Beach ('PHB'). An internet search of PHB led to news stories relating to the present proceedings involving the mother and the father. On 4 or 5 August 2020 Dr Marczak made contact with Mr Martyn Day, a London solicitor who was known to him.

26. Mr Day, in turn, made contact with Baroness Shackleton and informed her of his connection with Dr Marczak and the general area of Dr Marczak's work. He told Baroness Shackleton that Dr Marczak had identified someone at PHB as being possibly targeted by UAE directed spyware and that Dr Marczak had asked Mr Day to introduce him to PHB in order that, if they were interested, he would be able to advise them.

*(b) Mrs Cherie Blair CBE QC*

27. On the evening of the same day, 5 August 2020, Mrs Cherie Blair CBE QC received a telephone call from a senior member of the management team of NSO Group. Mrs Blair apparently acts as an adviser to NSO on business and human rights matters. Two witness statements from Mrs Blair have been filed in these proceedings. Mrs Blair states that the call from NSO in Israel took place at nearly midnight Israeli time. She was told that 'it had come to the attention of NSO that their software may have been misused to monitor the mobile phone of Baroness Shackleton and her client, Her Royal Highness Princess Haya.' The NSO senior manager apparently expressed great concern. Mrs Blair was told that NSO had taken steps to ensure that the identified phones could not be accessed again by their software. The NSO manager asked Mrs Blair to help in contacting Baroness Shackleton.
28. Mrs Blair was able to obtain the phone number for Baroness Shackleton and she made contact with her that evening. Again, it will be necessary to turn to more detail within Mrs Blair's evidence at a later stage.
29. It is, therefore, part of the mother's case that Baroness Shackleton was alerted to the possibility of phone hacking by two entirely separate mechanisms on 5 August 2020. The one, Dr Marczak, investigating signs of the consequence of any attempted hacking and the other, from NSO Group, originating from its source.

Dr Marczak as 'an expert witness'

30. Understandably the mother and those acting for her readily accepted Dr Marczak's offer of further advice and assistance in investigating the possibility that there had been phone hacking. Shortly after 5 August, Dr Marczak examined a number of phones said to be used by the mother and her staff, together with phones used by Baroness

Shackleton and others at PHB. He examined system diagnostic data ('sysdiagnose') from each phone together with the internet usage logs taken from the routers at the mother's London home and her home in Berkshire.

31. As a result of his investigation Dr Marczak produced a forty-two page 'witness statement' dated 7 September 2020 in which he concluded 'with high confidence' that the phones of the mother, Baroness Shackleton and Nicholas Manners (another solicitor, and since December 2020 a partner, at PHB) had been hacked by a single operator of NSO Group's spyware. On the basis that any such operator would be a nation State he concluded 'with medium confidence' that the government in question is the UAE Government. Further, there was evidence that the phones of the mother's Personal Assistant and two others on her staff had also been hacked.
32. The mother issued her application to this court seeking findings of fact on 7 September 2020. It is thus the case that Dr Marczak did not enter the proceedings in the manner conventionally used for the obtaining of expert evidence. He was not formally instructed in the manner required of the procedural rules before he began his work and by the time he had produced his written statement he had engaged in extensive and detailed communication with the mother, her security staff and those at PHB. Whilst, given the sequence of events that I have described, and given the need for the mother and her advisers to have the assistance of bespoke expertise in this narrow area of computer science, it is understandable that Dr Marczak entered the process and the application of the fact-finding were made in the way that they were and in the sequence that they were, that state of affairs generated a need for the court to adopt a careful strategy permitting the mother to deploy and rely upon the evidence of Dr Marczak, whilst, at the same time, conducting a process that was fair to the interests of the father and the children. In addition the process adopted was aimed at allowing the court to test the evidence which, at the start of the process, came from one source, Dr Marczak, supported at that stage to a degree by non-specific hearsay evidence originating from NSO and reported to the court subsequently in the statements of Mrs Blair.

### **Procedural Decisions**

33. I have taken time to describe the procedural and evidential landscape as it existed prior to and at the time of the mother's application for a further fact-finding hearing in order to make sense of the procedural steps that were then undertaken which were as follows.
34. In order to meet the unusual circumstances generated both by the method by which the evidence was introduced into the proceedings, and by the scientific complexity and sophistication of its content, it was necessary for the court to consider a range of procedural steps with the aim of achieving a fact-finding process that was both viable and fair to all the parties. These included the following:
  - (a) appointment of a confidential scientific adviser to the father and his legal team;
  - (b) appointment of an independent Single Joint Expert ['SJE'];
  - (c) communication between the court and NSO Group;

(d) appointment of independent counsel to review the extent of disclosure/redaction of all communications between Dr Marczak, the mother, her staff and her legal advisers;

(e) appointment of a second independent counsel to review information about Mr X;

(f) the presentation of the father's case.

35. I propose to describe each of these steps in turn.

*(a) Instruction of a specialist scientific adviser to the father*

36. During a case management hearing on 6 October 2020, Lord Pannick QC, leading counsel for the father, sought permission for the instruction of a cyber-security expert to advise the father and his lawyers on a confidential basis. In the circumstances, the application was not actively resisted by the other parties and permission was given. I dealt with the issue shortly in one paragraph in my judgment on that day:

“So far as the father being able to instruct his own privileged expert for the purposes of informing him and his team of the technical aspects, there is really no objection to that. I give that course my blessing as a wholly exceptional course taken in these proceedings, because the nature of the question to be considered by any such expert is wholly outside the comprehension of any ordinary human being and can only really be understood by someone of immense and particular experience and knowledge.”

37. Paragraph 15 of the order of 6 October set out the basis upon which permission had been given:

“Subject to the following conditions the father shall have permission, in the wholly exceptional circumstances of this case, to obtain advice from an expert or experts on cyber security on a privileged basis for the purposes of considering Dr Marczak's witness statement. The conditions are:

a) The name of the expert(s) must be made known to the court and parties before the instruction is effected;

b) The expert(s) must provide an undertaking (in like form as provided by the father's expert on security costs) to the court as to confidentiality prior to receipt of any papers;

c) The statement of Dr Marczak dated 7 September 2020 but no other court document may be disclosed to the expert(s). The statement may be provided in unredacted form save that all redactions as to the phone names, phone individual and phone numbers should remain redacted;

d) None of the data supplied to Dr Marczak for analysis shall be supplied to the expert(s).

e) Permission to the father to apply to the court in relation to c) and d) above for the restrictions to be removed or varied.”

38. The appointment of a shadow technical adviser to the father, whose advice and opinion were not required to be disclosed into the proceedings, was a wholly exceptional step. It was in part justified by a need to level up the forensic playing field in the early stages of the case during which the mother had open access to expert advice from Dr Marczak, yet the father had none. In the light of the highly technical content of Dr Marczak's statement, it was important that the father and his advisers should have their own source of specialist advice to enable them to understand the detailed content of Dr Marczak's statement and to be advised upon it.
39. At all stages, and on a number of occasions, the court has made it plain to the father that it would favourably consider an application by him for the instruction of his own expert witness, but that that instruction would have to be on the ordinary basis involving full and open disclosure of both the process of instruction and any resulting expert opinion. The father has at all times declined to make such an application.
40. The father instructed a firm based in Israel, Sygnia, as the special technical adviser for which permission had been granted to him. Despite the clear boundaries upon the extent of that instruction established by the court's decision, Lord Pannick QC has consistently pressed for the disclosure of the core data in the form of sysdiagnose files extracted from the phones of the mother, her staff and her solicitors, together with the records of network logs and Dr Marczak's own records of IP addresses, domain names and applications which he asserts are relevant to the Pegasus software. Lord Pannick has been plain that the purpose of disclosure was not to inflate the status of Sygnia into an expert whose opinion would be open to the court and filed in the proceedings. Lord Pannick nevertheless asserted that it is a basic requirement of fairness for the father's adviser to examine the core material upon which Dr Marczak's opinion was based in order to provide confidential advice to the father and his lawyers.
41. The court has consistently refused the father's applications in this regard. Although subparagraph (e) of the order granted permission to the father to apply to vary the embargo upon disclosure, I have been clear that the unprecedented relaxation of the long established approach to the open instruction of expert witnesses, whilst necessary and proportionate at the time that leave was given in this case, should not be extended further. Refusal was justified firstly as a matter of ordinary principle, but secondly because, by then, the court had embarked upon the instruction of a SJE and thirdly because the father was fully able to apply for his own FPR 2010, Part 25 compliant expert witness, but chose not to do so.
42. The father's access to, and receipt of advice from, Sygnia has, so far as the court is aware, continued throughout the trial process. It was no doubt available to inform the questions raised by the father's legal team during the instruction of the SJE and at the expert's meeting. It was also available to inform the lines of questioning during the extensive cross-examination of Dr Marczak.

*(b) Single Joint Expert*

43. Finding a source of expertise with sufficient knowledge and experience to act as a SJE on the question of whether or not the Pegasus software had been deployed to hack the phones of the mother and others proved to be a most difficult task. The endeavour was no doubt complicated by my insistence that it should be taken in stages, with the expert

only being exposed to Dr Marczak's statement at the second stage, once they had conducted their own examination of the sysdiagnose files and other core data.

44. The first SJE that was instructed, IntaForensics Ltd, undertook the first stage of investigation and reported that there was no sign that any of the relevant devices had been the subject of surveillance. I pause there to observe that, if it is the case that any of these phones have been infiltrated by Pegasus software, it is no surprise that a search for viruses, spyware or malware produced a 'nil' return as a principal selling point of Pegasus is said to be that it leaves no trace.
45. However, when Dr Marczak's statement was disclosed to IntaForensics they quickly responded indicating that they were unable to continue with the instruction. This message was followed up in a report dated 16 March 2021, which stated that the findings in IntaForensics' previous reports should not be relied upon. The report confirmed that the unusually named apps identified by Dr Marczak and the behaviour observed in these apps attempting to access standard features on the phones had been observed by IntaForensics. There was evidence that five of the six phones may have been the subject of surveillance and/or interference from an unidentified source.
46. The court is grateful to IntaForensics for taking up the instruction and being prepared to act as the SJE in this case. Because of the staged level of disclosure that the court insisted upon, IntaForensics were not to know the scale and character of the task for which they were being recruited and they command the court's respect, rather than criticism, for flagging up their inability to complete the instruction as soon as the situation became clear.
47. Fortunately, it was possible to identify a replacement SJE who was able to take up the instruction and respond quickly within the court's wider timetable. The expert instructed was Professor Alastair Beresford, who is Professor of Computer Security at the Department of Computer Science and Technology in the University of Cambridge. Professor Beresford's research work examines the security and privacy of large scale networked computer systems, with a particular focus on networked mobile devices such as smartphones, tablets and laptops. He has worked on mobile computing platforms in either industry or academia since 1995.
48. Before his instruction Professor Beresford was told that the court was interested in understanding whether or not the phones concerned had been infiltrated by the Pegasus software and that the court had received expert advice from Dr Marczak (whose general work was known to Professor Beresford). Professor Beresford was not given access to Dr Marczak's statement at that stage. Following his initial report which, like that of IntaForensics, confirmed that there was no trace of the Pegasus software on the sysdiagnose files or network logs, Dr Marczak's statement was then disclosed to Professor Beresford and there followed a short period of written communication through further written statements or reports orchestrated at the court's direction and culminating in an expert's meeting conducted by Ms Melanie Carew of Cafcass Legal and at which questions submitted by all three parties were addressed by Dr Marczak and Professor Beresford.
49. Professor Beresford gave oral evidence at the fact-finding hearing and was cross-examined by counsel on behalf of both the mother and the father.

*(c) NSO Group*

50. A full account is given of the involvement of NSO Group in the proceedings at paragraph 94 to 110. In terms of process, during October and November 2020 the court made directions requesting NSO to provide an account of the investigation that it had assured PHB it was carrying out. In the event a letter dated 14 December 2020 was sent to the court, via CAFCASS, by NSO. The relevant content of this letter is described at paragraphs 102 to 105. Since receipt of that letter no party has applied for a direction seeking to engage further with NSO either by way of requesting additional information or otherwise. On the first day of the fact-finding hearing Lord Pannick suggested that NSO might be asked a narrow and specific question arising out of the letter that had been received over three months earlier. This was expressly a ‘suggestion’ and not an application for a direction. After observations from the court as to a possible wider question that might be asked of NSO, the suggestion was not pursued.

*(d) Independent Counsel*

51. In early December 2020 PHB disclosed details of the extensive communication that had taken place between the mother’s staff and PHB with Dr Marczak. The communication, which was largely in the form of emails, text messages or other electronic communication, when committed to paper ran to some 900 pages. Whilst much of the content was open to be read, there was, nevertheless, a very substantial element that had been redacted. Basic codes had been attributed to each redacted section indicating the general reason said to justify non-disclosure. Whilst the father’s legal team accepted that some redaction was justified, for example withholding the names of security staff or an individual’s telephone number, they questioned the extent of the redaction that had been undertaken and the range of categories relied upon.
52. Following full submissions from all parties, the court determined that the redaction process should be audited and checked by a senior member of the Bar, who had been security cleared for instruction in other cases as a special advocate, and who would act as independent counsel for this purpose (see judgment [2021] EWHC 156 (Fam)).
53. The court is grateful to Jennifer Carter-Manning QC for taking up instruction as the independent counsel and for the diligent manner in which she has plainly discharged her instruction. Whilst the arrangements put in place by the court allowed for any dispute between the independent counsel and PHB to be referred to me for final determination, in the event all matters were resolved without the need for my involvement. The result was that a substantial number of redacted passages were opened up and disclosed to the father’s legal team, albeit only a few working days before the start of the hearing. This material was referred to extensively during cross-examination of Dr Marczak on behalf of the father.

*(e) Mr X*

54. Mr X, who features in Dr Marczak’s analysis on the basis described at paragraph 24 above, is of relevance for two separate reasons. Firstly, irrespective of his underlying identity, Dr Marczak asserts that Mr X’s telephone was targeted by Pegasus in a way that revealed the deployment of version 3 or version 4 IP addresses and the second fingerprint, domain names and apps that he attributes to Pegasus. The alleged hacking of Mr X’s phone happened in precisely the same time window at the end of July and

early August as the asserted infiltration of the phones relevant to these proceedings. Mr X is therefore directly connected to Dr Marczak's analysis on the first question of whether or not the mother's and other phones in this case have been hacked. Secondly, Dr Marczak asserts that Mr X is a known 'UAE activist' and that the fact, as Dr Marczak asserts is the case, that his phone was hacked by Pegasus and that the same State operator was involved in hacking Mr X's phone and also the phones of the mother and those connected with her is, claims Dr Marczak, of relevance in attributing the identity of the hacking to the UAE.

55. The father has consistently sought an order requiring the disclosure of Mr X's identity. Dr Marczak is unwilling to disclose it without Mr X's consent. The mother contends that Mr X should be told who the parties are to these proceedings before he is asked whether or not he consents to the disclosure of his identity to those parties. The father refuses to agree to the disclosure of his identity to Mr X. There was, therefore, a standoff.
56. The court has no knowledge of the identity of Mr X over and above that which is stated in Dr Marczak's written statement. It is therefore simply not possible for me to assess what risk, if any, might open up for Mr X were his identity to be disclosed to the father and his advisers in the UAE were I to direct it. Whilst, at one end of the spectrum, disclosure may have no consequence for Mr X, at the other it is possible to contemplate exposing him to actions which might engage rights under Article 2 or Article 3 of the European Convention of Human Rights. Being mindful that Mr X's identity is irrelevant to the first question, namely whether hacking has taken place, which turns entirely on technical evidence, and given my preliminary view that Mr X's involvement and what is said about him can only be of peripheral probative value on the second question of attribution, I have consistently refused to require his identity to be disclosed into the proceedings. However, in order to at least provide some check on Dr Marczak's assertion that Mr X is 'a UAE activist', I sanctioned the instruction of a second independent counsel, Gareth Weetman, who was tasked with undertaking a search via Google and other public source material to see what was said about Mr X.
57. The court is most grateful to Mr Weetman for undertaking this role. He has provided a schedule recording each reference that he was able to find to Mr X and I will turn to that material in due course.

*(f) The Father's Case*

58. In contrast to the first fact-finding hearing, where the father instructed his lawyers to vacate the courtroom and play no part in the process, the father has been represented throughout the current process by a very substantial legal team of the highest quality. On the question of jurisdiction, the issue relating to FAS was pursued to a full appeal and an application of permission to appeal to the Supreme Court. In addition, the court has heard applications upon, and made determinations about, a wide range of procedural matters raised by the parties. None of the court's determinations has been the subject of an appeal.
59. Unusually in a fact-finding process, and in contrast to the first fact-finding hearing, the father has chosen not to file any evidence whatsoever on the issues. The only material filed on behalf of the father is open source media and other articles to which the court has not been specifically taken other than via limited reference during cross-

examination. In addition the court has received position statements and skeleton arguments which put the mother to proof of the allegations and which, from time to time, have made varying suggestions as to other States that may be responsible for any hacking that may be proved, other than the father or those acting on his behalf.

60. In his skeleton argument for the fact-finding hearing under the heading 'The father's response to the mother's allegations' it is asserted that 'the mother has not established on the balance of probabilities', the following matters in particular:

- that there has been surveillance of the relevant mobile phones,
- that such surveillance was carried out using NSO software,
- that such software was licensed to the UAE or Dubai,
- that the surveillance was carried out by the UAE or Dubai,
- that the alleged technical capabilities of the NSO software are established, and
- that the alleged surveillance occurred with the father's express or implied authority.

The case has been conducted on the basis that the father can neither confirm nor deny that the UAE (including Dubai) has or had any contract with NSO for the supply or use of the Pegasus system.

61. In circumstances where the father has filed no evidence at all in response to the allegations, where he has not sought leave to instruct his own open court expert, where there is effectively no substantial dispute between the evidence of Dr Marczak and that of the SJE and where the father does not seek to put forward a positive case before the court (other than to make various and varying suggestions), it might be possible to justify closing down or severely limiting the father's ability to contest the factual allegations. At this hearing, however, the court adopted the contrary course. Lord Pannick was permitted full and equal range to that attributed to Mr Geekie QC and the mother's legal team to advance arguments prior to the hearing and in closing submissions. Most importantly, Mr Andrew Green QC, on behalf of the father, conducted an extensive, most thorough and professionally adept cross-examination of Dr Marczak which was spread over two days and lasted at least seven hours.

### The previous fact-finding judgment

62. The first fact-finding judgment, given in December 2019, made wide ranging findings against the father. These included the forced abduction of one of the father's older daughters, Princess Shamsa, from England in 2000 by those acting on behalf of the father, the restraint and house-arrest of another daughter, Princess Latifa, in 2002 and in the years following, the capture and forced return to Dubai of Princess Latifa from a boat in international waters off India by Indian Special Forces and the Dubai military in 2018 and her subsequent house-arrest, a campaign of fear and intimidation against the mother prior to her departure from Dubai in April 2019 and the campaign of harassment and threats that continued once she had arrived in England.

63. At paragraph 181 of the judgment I concluded that the findings established a consistent course of conduct by the father and those acting for him, over the course of two decades, 'where, if he deems it necessary to do so, the father will use the very substantial powers at his disposal to achieve his particular aims'.
64. It is not necessary to set out the earlier findings in more detail here, but before moving on from reference to the first fact-finding hearing it is necessary to correct a statement made by the father following the judgment in December 2019 and issued by his solicitors, Harbottle and Lewis. The father stated:

'As Head of Government I was not able to participate in the Court's fact finding process, this has resulted in the release of a "fact-finding" judgment which inevitably only tells one side of the story.'

That statement was at least disingenuous. It did not give a true account of the father's position before the court where, despite his position as Head of Government, the father had filed two full witness statements, where others named by the mother as being implicated could have given evidence on his behalf, and where he was represented by a large legal team who could (as at the present hearing) have been deployed to cross-examine the mother's witnesses and make submissions, but who were, on the father's instructions, simply withdrawn from the courtroom.

### Fairness

65. Having described the various features of these proceedings which are to varying degrees unusual, it is possible to make the following observations as to fairness:
- a) every single piece of evidence that has been admitted into the hearing has been fully disclosed to the father and his team. I, as the judge, have not seen any evidence that the father's lawyers and those acting for the children have not also seen. In so far as material has not been admitted into the hearing and has been withheld from disclosure to the father, it is not evidence in the case and forms no part of the material upon which I will make my decision.
  - b) In so far as Dr Marczak has examined and commented upon electronic data which has not been disclosed to the other parties and the court, that data has been fully examined and checked by both IntaForensics and Professor Beresford who, subject to minor corrections, have confirmed its accuracy.
  - c) In so far as Dr Marczak has relied upon data drawn from his investigations over the past five years and more, that data (including the 'second fingerprint') has been disclosed to Professor Beresford who, in turn, has reported upon its validity and accuracy in his evidence.
  - d) In so far as part of the content within the extensive records of communication between Dr Marczak and others relating to this case has not been disclosed to the court, the father or the children's guardian, that material has been fully considered and, where appropriate, challenged on the issue of disclosure by independent counsel instructed for that task.

- e) In so far as the identity of Mr X has not been disclosed to the father, the children's guardian or the court, details of his identity have been given to the second independent counsel who has conducted searches of public facing material and reported to the court.
- f) The father has at all times been able to apply to have his own openly instructed expert within the proceedings who would be instructed in accordance with the court rules and subject to the same stringent conditions as Professor Beresford.
- g) Despite having filed no evidence at all and having not put forward a positive case before the court, the father has continued to enjoy all the rights of a party to participate in the proceedings including making full submissions through counsel and conducting a thorough and extensive cross-examination of Dr Marczak.
- h) The fact-finding hearing, which was conducted entirely remotely over a Teams link, was open for the attendance of any UK accredited media representative. A number of media representatives attended throughout the hearing. In addition full transcripts of all of the interim and case management hearings which have taken place in the lead up to the fact-finding hearing have been made available for scrutiny by the media representatives.

#### Dr Marczak's written evidence

- 66. Dr Marczak is, on his own account, a computer scientist who has taken a particular interest in cyber security and covert surveillance. In particular he is the leading author of a series of articles published over recent years by 'Citizen Lab', an interdisciplinary laboratory based at the University of Toronto. The articles have sought to expose alleged abuses of spyware (in particular Pegasus) to target individuals (for example journalists or political activists). Dr Marczak's work in this regard has focussed on the Middle East and the UAE in particular. The father, rightly, submits that Dr Marczak entered these proceedings with a pre-established mindset and perspective on these issues. There is a danger, which I also accept, that Dr Marczak's goal was to establish that misuse of Pegasus software attributable to the UAE/Dubai had taken place. Lord Pannick, again rightly, submits that the court should be cautious both to avoid 'confirmation bias' in Dr Marczak's evidence and in the court's own approach to it.
- 67. Despite the unconventional route by which Dr Marczak's evidence has come before the court, I concluded at an early stage that it was right in these proceedings relating to children for it to be admitted. If the mother's case is right that her phone and those of others close to her have been hacked by this highly sophisticated surveillance software, it is almost inevitable that she would not know that this were the case unless either she were alerted by a whistle-blower within the operating organisation (which to a degree is her case) or she was alerted to the potential for hacking by an individual such as Dr Marczak who could only confirm the possibility that there had been hacking after he had examined all of the relevant devices and networks. In contrast to a more ordinary case where a party may make a factual allegation which is then investigated by an expert witness within the context of court proceedings, the mother in this case did not know

that she had an allegation to make until Dr Marczak had conducted his investigation and told her of his conclusions.

68. I have, however, been cautious to ensure that Dr Marczak is not regarded as an independent expert before the court. He comes to the court both as an individual who had reached his conclusions before the case commenced and one who is open about his interest in investigating covert surveillance activities which are attributable to the UAE. I have at all times been keen to follow and understand the science to identify such solid ground as there may be within it, rather than considering more general assumptions and assertions that Dr Marczak may make regarding the identity of the perpetrator.
69. Dr Marczak's evidence inevitably descended into a good deal of detail both as to the operation of the Pegasus software system and the various strategies that he has employed to detect it. Much of Dr Marczak's work in that regard is in the public domain. For that reason, for reasons of general public policy as to the disclosure of the workings of a system which is of importance to security services around the world and, most importantly, because it is not necessary to do so, I will not include such detail within this judgment.
70. I have already (paragraphs 20 to 23) described the basic method of investigation that Dr Marczak has developed to identify and track use of the Pegasus software over the years. I therefore turn to record the steps that he took once his invitation to assist PHB and the mother had been accepted in early August 2020.
71. Dr Marczak had noticed suspicious activity in mid-July and then again in early August on several devices used by Mr X. In particular he identified a number of domain names associated with IP addresses that he had previously identified as being connected with NSO in recent times ('version 4'). Also, the way in which Mr X's phones were made to communicate with the suspicious domain names, by sending a sequence of 'knocking' packets before it sent a request, rather than simply making contact, further suggested that covert surveillance was being undertaken. 'Knocking' in this sense is similar to a resident not answering the door to their home unless a knocker taps in a specific previously agreed pattern of knocks.
72. In addition, Dr Marczak observed that a number of unusually named applications ('apps') were active on the phones and were attempting to communicate with Pegasus command and control proxy servers. Dr Marczak assumed that these unusually named apps represented Pegasus spyware.
73. Initially, Dr Marczak provided PHB and the mother's staff with the IP addresses and domain names that he had observed on Mr X's phone as well as other IP addresses and domain names drawn from his wider research so as to enable those to be compared with data on the network logs at the mother's homes and at PHB. Dr Marczak then examined the sysdiagnose data from each of the relevant phones.
74. Examination of the phone attributed to Baroness Shackleton showed that an unusually named temporary app had connected with two IP addresses that were the same as those to which Mr X's phone had also linked. In addition the temporary app attempted to access three of the standard apps on the phone namely 'preferences', 'siri' and 'mail'. The 'mobile container manager' logs from Baroness Shackleton's phone also showed

several earlier cases where other apps with odd names had attempted to access the same standard apps on her phone without the user's permission.

75. The sysdiagnose from the phone attributed to Nicholas Manners showed that another unusually named temporary app had, between 3 and 5 August, attempted to communicate with six different IP addresses related to Pegasus domain names. Another temporary app had attempted to access the same three pre-installed standard apps on his phone together with a fourth one, 'notes'.
76. The network logs recording activity at the mother's Berkshire home showed that between 17 July and 3 August six attempts were made to access a particular domain name connected with Pegasus. Further, another Pegasus domain name and a further suspicious domain name uploaded 265 megabytes of data from the mother's phone. By way of illustration, that amount of data equates to some 24 hours of digital voice recording data or 500 photographs. It is a very substantial amount of data. Further, the sysdiagnose data from the mother's phone demonstrated that a temporary unusually named app had sought to communicate with the same four pre-installed applications as had been the case on Mr Manners' phone.
77. Signs of infiltration on the further three phones, namely those attributed to the mother's Personal Assistant and two of her security staff, were less specific in terms of directly connecting to Pegasus, however the same named temporary apps were found on those three phones and each of which had attempted to access the same pre-installed standard apps.
78. Dr Marczak stated his conclusions in his first witness statement as follows:

"I conclude that the following phones were successfully hacked by NSO Group's Pegasus spyware between the dates indicated. I have "high confidence" in this conclusion, which means that I do not believe there are any plausible alternative conclusions that could explain the data I have gathered. The phones may not have been under continuous surveillance during the entire period, as the Pegasus spyware is not necessarily "persistent", i.e. turning the phone off and on again may remove the spyware and necessitate re-infection. It is also possible that additional phones were infected, or that the following phones were also infected on prior dates and there is insufficient log data in the sysdiagnoses to establish this. [he then listed the six phones]

I conclude with high confidence that Nick Manners, Princess Haya and Baroness Shackleton were hacked by a single operator of NSO Group's spyware. I conclude with high confidence that this operator is a nation-state, because NSO Group's CEO asserted this in a sworn declaration and extensive reporting on NSO Group has yielded no evidence to the contrary. I conclude with "medium confidence" that the government in question is the UAE Government, meaning that I believe there are other conclusions as to the identity of the government that are within the realm of plausibility, but that the UAE Government hypothesis seems to be the most likely conclusion. The spyware

on the phones of Nick Manners, Princess Haya and Fiona Shackleton communicated with some of the same IP addresses and domain names as the spyware on Mr X's phone. Mr X is a UAE activist who was previously targeted by the same Pegasus operator that targeted Ahmed Mansoor, a well-known UAE activist, in 2016. The UAE Government is known to be a customer of Pegasus.

There is at present no technical evidence to suggest which government operator hacked the phones of Princess Haya's Personal Assistant [and the two unnamed members of her security staff] with Pegasus. However, given the lack of evidence of a second operator targeting individuals linked to Princess Haya, I conclude that it is more likely than not that these targets were hacked by the same operator as targeted Nick Manners, Princess Haya and Fiona Shackleton.

It is hard to say for certain what data Pegasus exfiltrated from the hacked phones, though according to a 2016 analysis of Pegasus, its capabilities included: tracking: tracking the targets location; reading messages including SMS and email, and from a variety of apps including iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype, Line, Kakaotalk, WeChat, Surespot, Imo.im, Mail.Ru, Tango, VK and Odnoklassniki; listening in on calls including phone calls, as well as calls placed through the WhatsApp and Viber apps; accessing the target's contact list, calendar, saved passwords, photos and other files, browsing history, and call logs; recording live activity by enabling the microphone; and taking screenshots and pictures through the camera."

79. Separately, Dr Marczak found that one of the phones attributable to the mother's security staff had a sysdiagnose which showed that on five dates in November 2019 three further Pegasus apps attempted to access software on the phone without success.
80. On 7 February 2021 Dr Marczak filed a second witness statement commenting upon the initial report of the first SJE, IntaForensics. It is not necessary to refer to the detail of that statement here. In a third witness statement dated 1 March 2021, Dr Marczak gave greater detail as to the process he had adopted when analysing the logs from the wifi system of the mother's home with particular reference to the phone that he understood was attributed to her. The statement included a table recording no fewer than eleven occasions when data had been downloaded and then uploaded between the mother's phone and destination IP addresses or domain names which Dr Marczak attributes to Pegasus. In particular, this includes the occasion already referred to when two hundred and sixty five megabytes of data was uploaded.
81. Dr Marczak's final witness statement, dated 28 March 2021 engages with specific points that had by then been raised by Professor Beresford. They are matters of detail and do not require recording here.

82. Finally Dr Marczak provided further information in two documents explaining his analysis of the purported targeting of Mr X's phone by Pegasus in 2015. In one of these documents Dr Marczak gives an extensive explanation of a method of calculating the approximate location of individual servers where the 'last-modified' header of an activity is either precisely the same, down to the last second, as GMT or is precisely and exactly a whole number of hours different (with no difference as to the minutes and seconds). Thus suggesting that the activity happened at precisely the same time, but was measured at a different clock time, precisely one hour different, because the clock of the proxy server was calibrated in accordance with local time in a different time zone. On the basis of this analysis Dr Marczak inferred that two of the suspicious Pegasus servers which appeared in links sent to Mr X in 2015 may have been run by the same Pegasus operator because all three IP addresses pointed to by these servers had a single inferred time zone of GMT+4 which is the time zone of the United Arab Emirates as well as other countries in that region.

**Professor Beresford: written evidence**

83. I have already set out Professor Beresford's academic post and his relevant experience in short terms at paragraph 47. In his first report dated 9 March 2021 he concluded:

"I have found no evidence that the iPhones in question have been the subject of surveillance and/or interference. This finding is not necessarily in conflict with those of Dr Marczak since I lack the technical details of how recent versions of the Pegasus spyware operate and manifest themselves as evidence in sysdiagnose files and in network logs. Access to further information on the operation of Pegasus from Dr William Marczak or another source may allow me to identify such evidence."

84. By the time of his second report, 24 March 2021, Professor Beresford had reviewed the overall methodology used by Dr Marczak as outlined in his three witness statements as well as in the core data that had been provided to him. He concluded:

"The overall approach taken appears sound and I have been able to confirm much of the technical detail."

85. Professor Beresford raised a number of detailed questions about precise entries and reference numbers in a small number of points recorded in the reports of Dr Marczak and Intaforensics. He sought clarification with respect to these various matters.
86. Professor Beresford described the proposed method of searching for command and control proxy servers as 'sound', however he observed it may produce incomplete results if connections from specific machines are blocked or techniques such as port knocking are required to elicit a response. Secondly, the method of scanning the entire internet is, he confirmed, 'a reasonable means to find servers which exhibit a response consistent with a C and C or installation server'. Professor Beresford had been sent underlying detail relating to Dr Marczak's 'version 3' fingerprint and he concluded that 'the overall setup used looks reasonable however a more detailed description of the method would be welcome.'

87. With regard to Dr Marczak's 'second fingerprint', details of which have been withheld from the court and the father's team, Professor Beresford said this:

"(Dr Marczak) also describes a second fingerprint which Dr Marczak has developed. I have been supplied with the technical details of this fingerprint. The method is distinct from the approach used for fingerprinting version 1, version 2 and version 3 Pegasus infrastructure. The idea proposed appears sound however I have some technical questions on the degree to which the new method might lead to false positives (asserting that an IP address is part of the Pegasus infrastructure when it is in fact not) as well as false negatives (failing to notice that an IP address is part of the Pegasus infrastructure when it is). My questions are perhaps best used as discussion points with Dr Marczak if this is permitted."

88. With respect to 'version 1' and 'version 2' Professor Beresford advised:

"The above methodology provides evidence that 'version 1' and 'version 2' responses were linked to NSO Group. While I have some outstanding questions in terms of checking the detail, the overall approach offers a route to demonstrate that the spyware installation intended for Mr Mansoor came from NSO group and therefore it is likely to represent their product Pegasus."

89. With respect to Mr X Professor Beresford was unable, on the information before him, to identify the domain name regarded as suspicious as being one connected to 'version 4' proxy servers.

90. In an addendum dated 28 March 2021 Professor Beresford confirmed that his investigation demonstrated that the methodology and more detailed arguments given by Dr Marczak on a discrete point in his second witness statement were sound. In a further addendum dated 4 April 2021 Professor Beresford returned to the topic of the 'second fingerprint' in the light of further information that he has been given. He concluded:

"The effectiveness of this technique rests on the fact that the fingerprint produced is distinguishing in the sense that it is able to detect all instances of Pegasus proxy servers (i.e. no false negatives) and does not accidentally claim unrelated services are Pegasus proxy servers (i.e. no false positives). Given the set of tests Dr Marczak includes, the range of possible variants is large. Having reviewed the fingerprint information and the data from the rest of the scan I am satisfied that the fingerprint is distinctive and therefore the rate of false positives or false negatives will be low."

91. Following the experts' meeting Professor Beresford provided a further final report on 9 April tying up a number of details and, in particular, concluding that there was good evidence linking Dr Marczak's 'version 2' and 'version 3' servers.

### **The experts' meeting**

92. An experts' meeting was held remotely on 6 April 2021. It was attended by Dr Marczak and Professor Beresford, and chaired by Melanie Carew of CAFCASS Legal. Detailed questions for the experts had been submitted by the legal teams for each parent prior to the meeting.
93. It is not necessary to rehearse the detail of this meeting, which included the resolution between the two experts of a number of matters of outstanding detail and resulted in a unanimity of opinion between them.

### **NSO Group**

94. I have already described in summary terms how the NSO Group first sought to make contact with Baroness Shackleton via Mrs Cherie Blair QC. It is now necessary to record more detail of the unchallenged evidence of the Baroness and Mrs Blair in this regard.
95. In her first statement to the court Mrs Blair stated that she received a telephone call on the evening of 5 August 2020 from 'a senior member of the management team of NSO', who she was specifically asked not to name. She states:

"I was told by the NSO senior manager that it had come to the attention of NSO that their software may have been misused to monitor the mobile phone of Baroness Shackleton and her client, Her Royal Highness Princess Haya. The NSO Senior Manager told me that NSO were very concerned about this and asked me to contact Baroness Shackleton urgently so that she could notify Princess Haya. The NSO Senior Manager told me they had taken steps to ensure that the phones could not be accessed again."

96. Mrs Blair was able to contact Baroness Shackleton and inform her of the information received from NSO. Baroness Shackleton told Mrs Blair that she had, on the same day, been contacted by a senior partner in another city law firm delivering a very similar message. After that call Mrs Blair spoke again to the NSO Senior Manager who 'confirmed that NSO had not contacted another city firm to approach Baroness Shackleton.'
97. Mrs Blair is clear that she has never been told the identity of the NSO customer suspected of carrying out this alleged surveillance. She does, however state:

"It had always been my assumption that 'the country' (or the government agency/security agency within this country) was Dubai. This is because I assumed no one else would have an interest in targeting Princess Haya and Baroness Shackleton. I have not had any explicit confirmation from NSO who their client was. However, during a conversation with the NSO Senior Manager, I recall asking whether their client was the 'big state' or the 'little state'. The NSO Senior Manager clarified that it was the 'little state' which I took to be the state of Dubai."

98. At this point it is right to explain that, in terms of a 'State', the Emirate of Dubai is a constituent member of the sovereign State of the United Arab Emirates. Dubai is not therefore a sovereign State itself, it is a federal state within the sovereign State of the UAE. Loose use of language, including by the court in the earlier fact-finding judgment and elsewhere, has at times referred to Dubai as a State, which, in the sense of a sovereign State, is incorrect. NSO's Chief Executive Officer has made it clear that it only enters into contracts to supply Pegasus software to sovereign States.
99. On 11 August 2020, Cherie Blair spoke again on the telephone with Baroness Shackleton at PHB. The call was attended by two other members of the family team at PHB. An attendance note of that call made by PHB has been shown to Mrs Blair who has confirmed that it is consistent with her broad recollection. She did not, herself, take notes of the call. The note states that during the call 'CB confirmed it was the Emirate of Dubai, not UAE in general, who she was talking about.'
100. On 28 August 2020, solicitors directly instructed by NSO Group (Schillings) wrote to PHB confirming that their client was 'investigating this matter' and could not confirm any factual information at that stage. A subsequent letter from Schillings, dated 1 September 2020, stressed that the identity of NSO clients is strictly confidential and that Mrs Blair was not privy to the identity of any of NSO's clients. The letter also stated that 'since 5 August 2020...onwards our client has no reason to believe that its technology is being or can be, deployed in the UK by any government agency against those identified in your letter, either by name or by reference to their roles. Whether there had been any breach prior to this is the subject of our client's investigation.'
101. In response to a direct request made by the court, NSO provided a letter, dated 14 December 2020, setting out an account of its investigation and subsequent actions. The court is grateful to NSO Group, who are outside the jurisdiction of this court, for responding to its request.
102. The letter includes general background information including the following:
- "NSO's purpose is to create technology which is licensed only to government intelligence and law enforcement authorities to enable those intelligence agencies and authorities to identify, investigate and prevent serious crimes and terrorism, and otherwise protect public safety.
- NSO is committed to aligning with the UN Guiding Principles on Business and Human Rights ('UN Guiding Principles'). Human rights protections are integrated in all aspects of NSO's work. Our desire to implement the highest ethical standards is demonstrated by NSO's detailed Human Rights Policy, and Transparency Statement of Principles, whereby we publicly report on the effectiveness of our policies and procedures.
- NSO takes its responsibility for ethics and accountability very seriously. The Human Rights Policy, Transparency Statement, and Whistleblower Policies feature prominently on our website and undergo constant review.

...

NSO does not condone, assist in or encourage the use of its software for purposes other than the agreed purposes specified and identified in the contracts it concludes with its customers on a lawful basis. Nor does it, or would it, agree with its customers to facilitate such use.”

103. The letter later moves on, under a heading ‘Relevant Background’, to give the following account:

“On 4 August 2020, NSO became aware of a possible use of the technology by a customer that was not in accordance with the contractual terms applicable to it, or which appeared to be beyond the purposes for which the technology was supplied... . As part of its review of this possible use, information was provided to NSO that raised the possibility that Baroness Shackleton's mobile phone, that of another unnamed member of her firm and that of her client (the Respondent Mother), may have been compromised. At this stage, NSO did not know the full facts of whether phones belonging to other individuals may have been compromised. We cannot reveal confidential information or the methodology by which NSO seeks to verify that its technology is used strictly in accordance with the contractual terms on which it is licensed, for the purposes set out above. To do so would prejudice NSO's capacity to investigate future incidents.”

104. The letter then gives an account of the investigation carried out by NSO before stating:

“The activity of gathering information for the purposes of the Investigation itself concluded on or around 15 September 2020, although the post-investigative process which NSO follows in order to make a final determination has only recently concluded. While the Investigation could not make any determinative conclusions as to what in fact happened, the recommendation following the Investigation was that the contract with the customer should be terminated, and that the systems which that customer had contracts for be shut down.”

105. The letter confirmed that the provision of services by NSO to the customer stopped completely as of 7 December 2020. In summary, the letter confirmed that, following its investigation, NSO had based its decision on the ‘working assumptions’ that ‘the customer acted in breach of its contract with NSO’ and that the phones of Baroness Shackleton, a member of her firm and the mother ‘may have been compromised’. The following is then stated:

“Following the investigation, NSO has not been able to establish any indication that the surveillance of the identifiers for (i) Baroness Shackleton and (ii) a member of her firm occurred prior to 7 July 2020. The investigation was also not able to

establish when the surveillance of the identifier for (iii) the Respondent Mother began.”

106. During the concluding section of the letter NSO confirmed that it was not able to reveal or confirm the identity of any of its customers. But it did confirm that ‘our products are used exclusively by government intelligence and law enforcement agencies’ and that therefore the father was not himself a customer.
107. That statement is consistent with a Declaration by Shalev Hulio, Chief Executive Officer of NSO Group, dated 16 April 2020, that has been filed in litigation in the USA. The court has seen a full copy of Mr Hulio’s Declaration which includes the following statement:

“NSO Group innovates cyber solutions that NSO Group does not itself use. NSO’s only customers are sovereign states and the intelligence and law enforcement agencies of sovereign states...”

A subsequent Declaration by Mr Hulio, dated 13 May 2020, sets out further details of the steps to which NSO Group goes to ensure that its product is used exclusively by sovereign governments.

108. It is of note that the dates given for the assumed compromise of the three phones to which reference is made accords with the evidence of Dr Marczak.
109. The court has seen a copy of NSO’s ‘Human Rights Policy’ dated September 2019. At a number of points the policy indicates the seriousness with which NSO will regard any serious misuse, or breach of contract by a customer. For example, paragraph xiii includes the following statement:

“After either our own investigation or a state investigation, if we have sufficient grounds to believe that our products may have been misused we promptly take appropriate action. Ultimately where necessary, we may suspend or terminate use of the product or take other steps that may be warranted.”

110. In the present case, as the NSO letter of December 2020 makes plain, after its investigation NSO has adopted the extreme remedy of terminating its customer’s use of the Pegasus software. In commercial terms, this step is to be understood as having great significance. The court has been given general information, but it is plain that the contract price flowing from a customer to NSO for access to and use of the Pegasus software is measured in tens of millions of dollars. Further, termination of a customer’s contract is likely, not only to affect the revenue flowing from the current licence term, but may well impact upon future revenue from that sovereign State in the years to come.

#### Mr X

111. Independent counsel, Mr Weetman, was provided with details of Mr X’s identity, including various spellings of his name in English and Arabic. Armed with this information he was able to identify some 30 or more references to Mr X via internet

searches; the number is approximate as there is some potential duplication between English and Arabic articles.

112. Dating is by reference to a year only and a distinction is drawn between [Year] and 'Recent'. Mr Weetman was not invited to clarify this distinction. I have proceeded on the basis that 'Recent' indicates current activity in 2021, but [Year] indicates activity which is clearly limited to that year. I have not assumed that 'Recent' activity only commenced in 2021; the reference is taken simply as indicating that it is current.
113. The distinction between 'Recent' and any entry for [Year] or earlier is of importance. All of the 'Recent' entries relate to articles connecting Mr X with interest in the affairs of [another state], whereas the earlier references, including [Year], refer solely to interest in the UAE and do not refer to any other State (save for one [Year] reference to the justice system in [another state]). Finally, one 'recent' social media site is recorded as including recent comments by Mr X, or highlighting comments by him, regarding alleged human rights abuses in [another state], UAE, [four other states].
114. The conclusion to be drawn from this material can only be that, insofar as he has publicly commented on matters, Mr X was, at least up until and during [Year], focussed on matters that were of concern to him in the UAE. More recently he has moved away from that focus and is now predominantly concerned with matters relating to [another state].

#### Dr Marczak: oral evidence

115. Dr Marczak gave oral evidence over a video link from California. The court sitting time was adapted as much as possible to accommodate the time difference, but the court is grateful to Dr Marczak for making himself available at an early stage on the two days over which his evidence was heard.
116. In response to the firm submission made by Lord Pannick that it was inappropriate for Dr Marczak to give any evidence in chief in the light of the very full and technically complicated statements that had been filed, Mr Charles Geekie QC's short opening questions for the mother were confined simply to matters of housekeeping. Ms Fottrell QC on behalf of the children's guardian had no cross-examination. Mr Geekie had no re-examination.
117. Dr Marczak gave oral evidence for over 6½ hours. This period was almost entirely taken up by cross-examination from Andrew Green QC on behalf of the father. It is right to record that Mr Green demonstrated cross-examination skills of the highest professional order. The structure of the cross-examination and the content of the questions were designed to test Dr Marczak's testimony across a wide canvas, including not only matters of technical detail but also possibilities of bias or fixed mindset against the UAE and Dubai. In addition Dr Marczak was questioned closely on the detailed communications that had been disclosed of discussions that he had had with the mother's security staff and others during the course of his investigation. The questioning was entirely justified and, given the unconventional route by which Dr Marczak had been introduced into the proceedings, the court benefitted greatly from having these matters tested in such detail by an advocate who plainly had total command of his brief and the skill with which to deploy that information in the best

interests of his client, the father. Save for one aspect that did not require further elaboration, I do not think that I intervened at any stage to restrain or direct Mr Green in the questions that he sought to put.

118. For his part, Dr Marczak also demonstrated, as might be understandable, a thorough grasp of the detail (both technical and factual) upon which his evidence was based. He gave clear answers to each of counsel's questions and in all other respects co-operated with the cross-examination process fully.

119. The following aspects of Dr Marczak's oral evidence are of particular note:

(a) He began monitoring Mr X's phone around January 2020. Mr X was one of a dozen or so other activists he was also monitoring. The UAE was not the only State of interest in the monitoring process. Other States including Bahrain, Saudi Arabia, Ethiopia, South Korea and Tibet.

(b) Dr Marczak has a working 'victims list' which is a list of leads towards investigation. The list identifies the IP addresses of supposed victims. The source of information leading to inclusion on the 'victims list' does not come from examination of sysdiagnoses or the identification of a server. It comes from elsewhere. Dr Marczak accepted that the identification of others who may be on the 'victims list' could be of relevance to these proceedings, but he was not prepared to disclose the list.

(c) There were IP addresses registered to Jordan on the 'victims list'. Dr Marczak accepted that this was not mentioned in his report. Dr Marczak confirmed that there were potential Jordanian targets on his 'victims list'. He was not able to recall the precise number, but thought it may be ten or twenty, but subject to quite a margin of error.

(d) Dr Marczak had had no communication with the mother or anyone acting for her before the 4<sup>th</sup> August when he made contact with Martyn Day at Leigh Day.

(e) Network logs for PHB were never examined and, on his understanding, were simply not available.

(f) Dr Marczak did not know anything about the history of the phones. He was simply given access to the sysdiagnose and the devices and told that these were the phones of named individuals.

(g) Dr Marczak accepted that the 'mobile container manager logs' went back many months on the phones. If the sysdiagnose files had been altered in any way deliberately, that would be hard to detect.

(h) Dr Marczak confirmed that the phones of the mother's Personal Assistant, and the two security officers did not contain

direct evidence of those phones trying to communicate with the Pegasus proxy server. The analysis nevertheless indicated that these three phones had been infiltrated was based upon the identification of distinct app names and the distinctive pattern of the security failure that exhibited in the mobile container manager logs for each of the phones that was similar to those which did communicate with Pegasus proxy servers.

(i) Dr Marczak referred to a distinctive pattern of entitlement failure which involved specific apps trying to access preferences, Siri and mail, but failing. For Dr Marczak the pattern of accessing only those apps, combined with the fact that the requesting app has an unusual name is 'quite distinctive'. Most of the apps seen on iPhones are installed, as they have to be, through the AppStore controlled by Apple. The names of these apps are totally different from the format of App Store app names. The unusual behaviour is a combination of the unusually named apps, trying to access the same three or four ordinary apps, and no other, and doing so immediately after they log into the phone. This behaviour was observed on all of the suspect phones.

120. Towards the end of the first day of oral evidence, and at the beginning of the second, Dr Marczak was questioned about his analysis of the network logs at the mother's Berkshire home. He had examined the network log at the mother's London home, but had found no material evidence and had not, therefore, referred to that log in his written statement. During the initial search of the Berkshire home network log Dr Marczak's invoice records that he 'reverse engineered...to extract dates and times at which four unidentified Pegasus victims called devices' at the home. It went on to state 'Goal is to ID these additional victims linked to the case'. Dr Marczak explained that these individuals could not be said to be 'identified'. At that stage he had simply identified an overlap between the proprietary information on his 'victim list' and communications noted on the mother's network logs to or from those named IP addresses. When first giving evidence about this he could not recall whether they had eventually been identified. He did not regard this as being a particularly important part of the process.
121. On further questioning Dr Marczak had not included this information in his written statements because the information was based on his 'list' and he did not wish to reveal the content of the list or its source. Because the provenance of IP addresses on the list may be variable, Dr Marczak did not 'feel comfortable' saying with any level of certainty 'look, there are these additional victims'. He accepted that, with hindsight, he might have referred to this in his statement.
122. In his evidence at the start of the second day Dr Marczak explained that he had a number of lists with Pegasus servers, or probable Pegasus servers, identified on them. There was a list drawn from Mr X. There was also a wider list of Pegasus servers and then there was a 'victims list' referring to the specific servers in this case. Only the 'victims list' has any detail about victims, the other lists show detail about IP addresses and domain names linked to Pegasus servers. When he had referred to Jordanian IP addresses at an earlier stage of his evidence, he had been referring to addresses on the 'victims list' associated with Pegasus servers linked to this particular case.

123. Dr Marczak confirmed that the home network log identified an IP address of a supposed Pegasus victim connecting with the mother's home network. As far as he could recall this data referred to one of the six phones on the list, but he could not be 100% sure.
124. Dr Marczak explained that the IP addresses that were seen on the home network log were not users of the home wifi system, they were IP addresses that were being communicated with, for one reason or another, from users inside the home. He therefore questioned the relevance of each of these links. He also questioned of how useful this information might be given that it might indicate a false positive or a false negative connected with the victims list. The firmer evidence, he suggested only came when one examined the phones and saw what was on the sysdiagnose. He therefore only referred to individual devices in his first witness statement if any earlier information was also confirmed by examination of the sysdiagnose.

**Professor Beresford: oral evidence**

125. Professor Beresford's written reports demonstrated a meticulous demeanour with a commendable obsession for detail which had enabled him to spot small typographical errors in various IP addresses, app and domain names (some of which are long and complicated) contained in Dr Marczak's various statements. This attention to detail was further demonstrated throughout his oral evidence. I formed the clear impression that he was an extremely careful witness who was keen not to say anything unless he had confidence in the accuracy of his answer.
126. Professor Beresford confirmed the contents of his reports by being taken to the specific headline points by Mr Geekie. In particular, with regards to the 'second fingerprint', he confirmed that he had had full access to it and had discussion with Dr Marczak about it. As a result he was satisfied that Dr Marczak had successfully identified the version 4 Pegasus servers.
127. Professor Beresford expressly confirmed Dr Marczak's analysis of the sysdiagnose from the six phones. He confirmed Dr Marczak's conclusion that the phones of the mother, Baroness Shackleton and Mr Manners showed infection by Pegasus as being 'a proper conclusion to come to'. And that a lesser degree of specificity applied to the other three.
128. Professor Beresford had the following exchange with Mr Geekie:

"Q To be clear, there are four phones, Mr X, Baroness Shackleton, Her Royal Highness and Mr Manners, that you are satisfied are infected with Pegasus software and it is the same operator?

A Yes, based on the material I have been provided with and the extra checks that I have performed, yes."

"Q There was also - you were satisfied because you could see the data for this - 265 megabytes of data were taken from Her Royal Highness' phone and communicated to a Pegasus server?

A Correct, that is what the logs I have been provided with show.

Q As you have acknowledged today and have acknowledged in your written reports, there are some, I would suggest relatively small, areas where, for reasons explained by you and Dr Marczak, it has not been possible for you directly to verify the steps taken by Dr Marczak?

A No, there are a number of areas where I am reliant on Dr Marczak. They include for example the provision of some of the data and that that data has been collected correctly, and there is an appropriate chain of custody around those data items, yes.

Q So in relation to that set of material, just concentrating on that set of material, you are satisfied as to the methodology he has applied, you just have not been able to look at the primary data yourself and followed it through in the way that you have in many other areas?

A Dr Marczak has often provided me with the primary data, so for example the data from ...(examples given)... of course I am still reliant on him having collected that correctly similarly with the sysdiagnoses I am reliant on those having been collected from the correct handsets and provided. A few other areas for example in the case of the analysis of the version 9 servers, the origin input files, the pcap files are not available. Given the time that has passed it is not possible for me to collect them again, so I am reliant on Dr Marczak there. There are a number of areas where we are reliant on his data collection process.

Q Yes, that is set out very clearly, both by you and Dr Marczak. Just to confirm, with that caveat in mind, so far as the methodology is concerned, you are content with the methodology he has applied?

A I am content with the approach taken, yes."

129. In cross-examination Professor Beresford confirmed that he had never been asked to look at the Pegasus system before or otherwise been involved with it. He had not conducted a full worldwide internet scan to check Dr Marczak's evidence on this point. He said that it would now, probably, not be possible to do so.
130. Professor Beresford confirmed that in his first report he had not identified the unusually named apps relied upon by Dr Marczak as not being issued by Apple. He accepted that maybe he should have seen them and if he had they would have struck him as odd.
131. Professor Beresford confirmed that he had conducted his own independent research around the data associated with Dr Marczak's 'version 1' servers. In his second report he had set out the reasons why he considered there were links to NSO Group. He also confirmed the existence of the link working backwards from version 4 through versions 3 and 2 to version 1.

132. It was explained that evidence of the presence of Pegasus software on a phone did not, of itself, establish that the person connected with that phone was the primary target of any surveillance operation or a subsidiary means of getting to a different primary target connected with that person who may make contact with them and has communications with them and could be observed when they did so. Professor Beresford responded:

“So, I guess there is evidence from multiple phones here. I guess if the centrepiece was somewhere else, then I guess the interesting question is: would you expect to see the same pattern of phones targeted in this case or not? So some other person let us call them ‘Mr Z’, so if Princess Haya was somehow related to Mr Z, would it also make sense for some of the other phones in this case that we have seen to also be targeted if the central focus was Mr Z or not?

...

So, one of the problems with this sort of line of reasoning is that if you compromise the people associated with the victim you get a lot less data. You are only going to get information if Mr Z is talking with the phones that you have hacked. Whereas if you want, for example, the archive of photos off the device, you are not going to get that via another third party. There are significant advantages for attempting to hack the actual target rather than associates.”

133. Following that explanation, Professor Beresford nevertheless accepted that he could not say that the mother in this case was the primary target from the information that he had seen.

### Conclusions

#### *(i) The Fact of Hacking by Pegasus software*

134. Having now referred in detail to the evidence, it is possible to set out my conclusion on the first issue, namely whether the six mobile phones of the mother, her solicitors and her staff have been the subject of unlawful surveillance, or attempts to achieve such surveillance, in July and August 2020 and that the means of surveillance, or attempted surveillance, was via NSO Group’s Pegasus software.
135. In approaching Dr Marczak’s evidence I have exercised a great deal of care. He does not come into the case as an expert in the conventional sense. He stepped forward to offer assistance to the mother and her team which they readily took up. It was only after that that he became a potential witness. The assistance that he gave meant that he was in very close communication with the mother’s staff and solicitors during his investigation. That route into the litigation does not render him automatically biased or irreversibly partisan, but it must be a matter for concern that that may be the case and it has therefore been a matter upon which I have maintained a keen eye throughout.
136. Further, Dr Marczak has an acknowledged interest in tracking the use of the Pegasus software by the UAE (including Dubai). He states that the episode in July 2020 that put

him on notice of this case, originated from his relationship with Mr X. He stated that he had reached the conclusion, before contacting Martyn Day, that Mr X's phone was being infiltrated by Pegasus and that, because of Mr X's interests as 'a UAE activist', this was likely to be via an operator in the UAE. To this extent, and it is an important factor, Dr Marczak does not stand above the fray. He is not a disinterested academic who simply monitors events from a distance, he is actively on the lookout for potential abuse of the Pegasus system. He is known as such to activists and, as evidence about Mr Mansoor and Mr X suggests, it is to him that activists turn if they are suspicious that they are being targeted. It is therefore entirely right that Lord Pannick advises the court to be on the guard for 'confirmation bias' in Dr Marczak's evidence.

137. Despite these important caveats and the justified need for caution, during the course of Dr Marczak's oral evidence I was progressively more and more impressed. His grasp of the detail of the Pegasus system and his own researches, previous encounters with it and published articles was to be expected, but it was, nevertheless, impressive and was maintained without significant falling off or error over the course of the two days. He was equally clear and firm in the detailed knowledge and recall that he had of his investigation for this case. He presented foremost as a scientist, who worked strictly within the confines of the data and the principles of computer science. His opinions, both micro and macro, were carefully built upon and supported by the data and the underlying engineering of the complex systems with which he works. I did not detect any occasion when he might be seeking to stretch the science to fit a pre-determined conclusion in relation to the fact of hacking and the identification of Pegasus software.
138. Despite being properly and thoroughly tested at every turn by the intelligent and probing questioning of Mr Green, Dr Marczak gave measured, clear and full answers to each question. Where there was a need to do so, he conceded matters or readily accepted corrections. As each stage of the cross-examination proceeded, I became more and more impressed with the witness.
139. Dr Marczak was, in short, an impressive witness who presented a detailed, logical account, supported by the core data that he had found, which led to the conclusion that there was strong evidence that the three principal phones had been hacked by Pegasus software and that it was probable that the other three phones, which exhibited some but not all of the suspicious features, had also been infiltrated. It is not necessary in this conclusion to go back through the detail that I have already set out, leading from Mr Mansoor to versions 1 to 4 and the second fingerprint. Despite very close analysis, there is no break in that chain which links the alien apps and the IP addresses found in the sysdiagnose and network logs in this case with the deployment of NSO Pegasus spyware.
140. The court has been most fortunate both to have located Professor Beresford and to find that he has been able to meet our extremely tight time-table. Whatever may be said about Dr Marczak's standing as an interested party and player in the relation to tracking down the use and abuse of Pegasus spyware, the same cannot be said of Professor Beresford, who has more than 25 years experience in the narrow field of computer security, but who comes to the Pegasus system having had no prior direct involvement with it. His independence from having any attraction to one outcome or another was clear, as was his expertise in this narrow and highly complex field. Professor Beresford adopted an approach to the case which demonstrated a meticulous attention to detail, and a need to have issues or assertions fully clarified before he was prepared to sign-

off on them and move on. That approach was amply demonstrated both in his written reports and in his oral evidence. I am fully satisfied that the court can place substantial weight on Professor Beresford's endorsement both of Dr Marczak's overall approach to this analysis and his detailed conclusions on the core data.

141. The evidence from Dr Marczak and Professor Beresford, which is supported to a degree by confirmation from IntaForensics, is based on detailed, logically developed, analysis which itself (in Dr Marczak's case) arises from research in this precise field going back over six or more years.
142. Dr Marczak has explained his process of analysis to the court in detail. He has been fully open with Professor Beresford in explaining what lies beneath it in computing terms and he has expressly disclosed details of his second fingerprint. After an apparently meticulous audit, and some research of his own, Professor Beresford has pronounced Dr Marczak's method and conclusions as 'sound' and he has found no reason to challenge them insofar as they establish hacking via the Pegasus software.
143. Separately, the court has the evidence from NSO, both in the form of the account given by Cherie Blair QC and in the NSO letter. It is clear from Mrs Blair's account that, from Day One, NSO had sufficient information that its software had been used against Baroness Shackleton and the mother to cause the senior management to take steps to make contact, during the night, to alert PHB that this was apparently the case. Thereafter NSO state, and I have no reason not to accept, that they undertook a full investigation, including visiting the customer State. Whilst the letter is written in careful terms, the 'assumption' that this hacking had indeed occurred was sufficient for NSO to terminate the customer's contract. That is a step which NSO documentation describes as only being taken 'ultimately where necessary'. It is a step with very significant commercial consequences for NSO and, I am entitled to assume, would only be taken if there was a clear basis for doing so.
144. There is a need for caution. The court cannot attach the weight to the NSO letter as would be open to it were the NSO investigator to have filed a full report with the court and been available to give oral evidence. To an extent, despite the letter, the court still looks at this side of the evidence through a glass darkly, hence my reference to the Delphic quality of the letter soon after its receipt. That said, it is a letter from a source which is extremely well placed to be able to say whether or not its software has been used, as it assumes has been the case. On its own, the letter might be sufficient to prove the first factual allegation. I do not have to determine that proposition as it is not on its own, it is but one part of the overall evidential picture on this issue.
145. Standing back, therefore, and looking at the overall picture, the evidence in favour of a finding of hacking comes from two distinct sources and travels in two separate directions. One source, the phones and network logs focus on evidence of the hacking event at the receiving end. The other source, namely that from NSO, involved an investigation of activity at the command and control, or sending, end. In their separate ways, using differing methods, both sources support a positive finding.
146. I see no reason to question the evidence and conclusions of Dr Marczak and Professor Beresford (supported by IntaForensics), on this first issue. That evidence alone establishes very clearly, and well beyond the tipping point of the balance of probabilities, that hacking by Pegasus of these 6 phones took place. That state of affairs

is fully supported by the evidence that has originated from NSO and goes further to strengthen the firmness of my conclusion on the first issue.

147. I therefore find that all six of these phones have either been successfully infiltrated, or at least the subject of an attempted infiltration, by surveillance software. I find that the software used was NSO's Pegasus software. In relation to the mother, it is clear that the attempt succeeded with a very substantial amount of data (265 MB) being covertly extracted from her phone. It is also probable, and I so find, that there was successful hacking of the phones of Baroness Shackleton and Mr Manners. The finding in relation to the other three phones is that there was an attempt to hack into them and that this was part of the same attack by Pegasus software as that affecting the principal three phones.
148. In setting out these findings I have used 'attempted' on a number of occasions. This arises because, unless there is evidence of data being transmitted from the phones, signs that alien software has been at work within them but, on a number of occasions, has 'failed' to connect with, for example, the 'mail' app, proves that there was a successful infiltration of the phone but does not prove that any data was actively extracted on those occasions. My understanding is that if the alien app is successful in accessing the phone's standard apps this event will not appear in the phone's memory manager log; thus only the failures are recorded. Thus, where I have used the word 'attempted' that is at least what has occurred, rather than the limit of the activity.
149. It is also necessary to explain that the sysdiagnose from the phones themselves do not apparently record whether any data has been extracted or not; the fact of connection with a proxy server is recorded, not the content of any transmission over that connection. Dr Marczak was able to say that on one occasion 265MB of data was extracted from the mother's phone because of records in the network log at her home, not from information on her phone itself. PHB did not have a network log at this time, hence it is simply not possible to know what and how much data, if any, was harvested from the phones of Baroness Shackleton or Mr Manners during this period.
150. Finally, in terms of clarifying matters, whilst the fact that 265MB can be stated as the amount of data taken from the mother's phone on one occasion, it is not possible to identify what this data was (save that it was a very substantial amount). The summary copied from Dr Marczak's report at paragraph 78 above describes just how wide the Pegasus software can reach in capturing an individual's personal data from a phone.
151. On the basis of those findings, and in further reliance upon the evidence of Dr Marczak, supported by Professor Beresford, I also find that one of the mother's security staff's phone had earlier been the subject of at least an attempt at hacking on five dates in November 2019.

*(ii) Attribution: who originated the hacking?*

152. Turning to the second and final set of findings, relating to attribution, the starting point is the firm and clear account from NSO that only a sovereign State, or the security services of a sovereign state, can purchase a licence to use the Pegasus software.
153. In the context of this case, as the Emirate of Dubai is not a sovereign State, Dubai could not, therefore, be the customer.

154. Moving on, standing back from the detail of the evidence and asking the question ‘who would have an interest in hacking the phones not only of the mother and her staff, but also (and at the same time) the solicitors who are instructed to represent her in these proceedings?’, the father and those acting for him in Dubai must fall for prominent consideration. No one has a closer interest in these proceedings than the two parents and the children. Whilst others, the Press, commentators, the general public may be aware of the case and may be interested in it, that interest is on an altogether different plane to that of the father and mother.
155. Although Dubai could itself not be the customer, the sovereign State of the UAE could be. The father is the Prime Minister of the UAE and Head of Government. The court is entitled to assume that the father and those acting for him must have the ability to instruct those in the security services of the UAE to take action on his behalf. The findings of fact previously made with respect to Princess Latifa establish that the father is prepared and able to use the government security services for his own family needs, and that this has occurred in the recent past. When one adds the father’s natural and proven interest in these proceedings, which far outweighs anyone’s save for the mother and the children, to the need for the perpetrator of the hacking to have access to the levers of control in a sovereign State sufficient to order its security services to act on his behalf, the prospect that it is the father comes yet more clearly into focus.
156. Lord Pannick, at preliminary hearings, has raised the prospect that the court may be in the position of contemplating a number of potential originators of the hacking. The court has been reminded that an individual may only be considered as a potential perpetrator if there is a ‘real possibility’ that this is the case. The father’s case is, however, that if there is a pool of perpetrators then the evidence is insufficient for him to be in that pool. In other words that there is no ‘real possibility’ that he is the originator. It is a submission that has been repeated on more than one occasion. It is one that I find is impossible to accept. In the circumstances of this case, it is beyond contemplation that the court, or indeed any rational person acquainted with the facts, could say that there is no ‘real possibility’ that the father originated the hacking of his former wife, her staff and her lawyers. No conclusion other than that there must be a real possibility that it is him is tenable.
157. Establishing a ‘real possibility’ is not, however, the relevant test of proof. It does not establish a pseudo-burden of proof on the father to point to someone else. The right question, as Peter Jackson LJ identified, is ‘does the evidence establish that the individual probably’ acted as it is alleged that he did.
158. I do not place any reliance upon evidence from Dr Marczak on the issue of attribution. On that issue, however, it is necessary to evaluate the degree of weight, if any, that can be attached to what is said about Mr X.
159. For the reasons that I have already given, I accept Dr Marczak’s evidence that the indications of hacking activity on Mr X’s phone in July 2020 are of a piece with that found on the phones in this case. I also accept his evidence that NSO issues each of its customers with access to separate, bespoke, proxy servers. I am satisfied that the proxy servers with which Mr X’s phone was communicating were replicated on the phones in England. I am therefore satisfied, on the balance of probability, that Mr X, the mother, her staff and her solicitors were all subject to infiltration from the same State government’s operation of Pegasus software.

160. The independent counsel's internet searches regarding Mr X have limited probative value. The court does not itself know anything of Mr X and must be cautious. With those caveats in mind, the independent counsel's researches do indicate that, until recently, and certainly during [Year], Mr X continued to demonstrate an established critical interest in human rights and other activities within the UAE and that he was not, at that stage, publicly interested in the activities of other States. The hacking took place in July or August 2020.
161. To a degree it is possible to make a case, and Mr Geekie seeks to do so, that late July 2020 was a particularly busy and financially interesting time in these proceedings, with the build up to key hearings relating to the mother's long-term financial claims for herself and the children. I am not, however, able to put any weight on this factor. Dr Marczak's evidence demonstrated that the Pegasus software is to a degree opportunistic in the sense that it will become very active, and will capitalise upon, the haphazard opening up of gaps in the security software protecting phones which lead to 'exploits' arising which, as that label suggests, are then exploited. It is also clear from Dr Marczak that he had observed a good deal of Pegasus activity in this very period and was trying to check out a range of potential 'victims'. That is how he found PHB and became connected with this case. I do not therefore consider that the date of the hacking arises from the fact that there was something of interest in July to gain information about in this case; rather the opening up of an exploitive window gave the operators the chance to do so, which they plainly took.
162. Whilst the father does not have to prove anything, it is the case that he has chosen not to attempt to do so. The court does not therefore have any evidence to put in the balance against a finding that the originator was the UAE on his authority. That state of affairs does not, I repeat, prove the case; it is simply an acknowledgement that there is no evidence to the contrary.
163. What the father has done is to float various suggestions before the court to the effect that another sovereign State is, or may be, the originator of the hacking. These have changed from hearing to hearing. At various times the states of Iran, Israel and Saudi Arabia have been suggested. In the main hearing itself, the suggestion being pushed was that it may be the State of Jordan. In the past Lord Pannick has proffered the idea that it would be in the interests of another State to undertake the hacking in order for the mother and for the court to jump to the conclusion that the father was the culprit. The purpose, it was suggested, of this subterfuge being to embarrass the father and thereby somehow further the interests of the originating State. Nothing was said as to the mechanism by which the mother or the court might find out that this highly sophisticated software had been used against her, or why another State might risk losing its very valuable contract with NSO, in order just to embarrass the father in this way even if NSO ever discovered that hacking had occurred. These various propositions were not pursued at the final hearing.
164. The suggestion now, very lightly laid out in cross examination and submissions, is that the State of Jordan may be responsible. The fact that Dr Marczak's 'victims list' may contain 20 or so Jordanian IP addresses and the possibilities that it may be that some unidentified individuals may have communicated with the mother's home using hacked phones and that they may be Jordanian, are referred to. The current apparent political and familial unrest in the ruling class in Jordan is also referred to.

165. These shifting suggestions, none of which is backed up by any evidence, are so insubstantial as to be without consequence in the evaluation of the question of attribution. If the standard of proof were 'beyond reasonable doubt', they might have some traction, but to my mind, where the standard of proof is the balance of probabilities, they have none.
166. One small piece of evidence, which is unchallenged, is Mrs Blair's account in her statement for the court of her conversation with the NSO senior manager:
- "However, during a conversation with the NSO Senior Manager, I recall asking whether their client was the 'big state' or the 'little state'. The NSO Senior Manager clarified that it was the 'little state' which I took to be the state of Dubai."
- This evidence, like others, should not carry more weight than is reasonable, but it is a considered account in a witness statement from a source upon which the court is entitled to rely for care and accuracy on a point such as this. It proves, as I find, that the NSO manager did speak in this way and refer to the 'little state' as opposed to the 'big state'. That conversation is compatible, and I place no greater reliance upon it, with the two 'States' being Dubai within the bigger State of the UAE.
167. Drawing these matters together, of those to which I have referred, I regard two elements of the overall evidential canvas to be of particular weight.
168. Firstly, it is obvious that the father, above any other person in the world, is the probable originator of the hacking. No other potential perpetrator, being a person or government that may have access to Pegasus software, can come close to the father in terms of probability and none has been put forward other than via transient and changing hints or suggestions.
169. Secondly, as the previous findings of fact establish, the father, who is the Head of Government of the UAE, is prepared to use the arm of the State to achieve what he regards as right. He has harassed and intimidated the mother both before her departure to England and since. He is prepared to countenance those acting on his behalf doing so unlawfully within the UK.
170. The evidence concerning Mr X and from Mrs Blair is entirely compatible with, and is not contrary to, a conclusion that the source of the hacking was the UAE.
171. The previous findings of fact and the evidence adduced at this hearing, as I have described it, taken together are more than sufficient to establish that it is more probable than not that the surveillance of the six phones that I have found was undertaken by Pegasus software was carried out by servants or agents of the father, the Emirate of Dubai or the UAE and that the surveillance occurred with the express or implied authority of the father.

### **The children's welfare**

172. Having stated my conclusions on these factual matters, the focus of the court will, at last, turn fully to the welfare of the two children. In this context, I note that in a Position Statement dated 2 October 2020 the father stated that 'it is hard to see how the hacking allegations make a substantial difference' to the issue of the father's contact with the

children. The court will return to this aspect in detail at the welfare hearing, but to assist the father at this stage I wish to make it plain that I regard the findings that I have now made to be of the utmost seriousness in the context of the children's welfare. They may well have a profound impact upon the ability of the mother and of the court to trust him with any but the most minimal and secure arrangements for contact with his children in the future.

173. It does not take long to contemplate just how an individual would react to discovering that their personal phone, and those upon whom they rely for confidential advice, support and protection, have been infiltrated by the most sophisticated spyware that is available, and to know that a very substantial amount of personal data has been stolen, yet not knowing precisely what. It is often said that the most important thing that a house-burglar steals is the peace of mind of the householder. The same must surely be true of phone hacking.
174. The court has, on many occasions, stressed to the father since the start of these proceedings that the most important goal should be to build up 'trust', so that the mother and the court, and indeed the children, can trust him – in particular trust him not to take unilateral action to remove the children from their mother's care. The findings made in this judgment prove that he has behaved in a manner which will do the opposite of building trust. The findings represent a total abuse of trust, and indeed an abuse of power, to a significant extent. It is an abuse which has been compounded by the manner in which the father has contested these allegations and instructed his lawyers. Despite the weight of evidence, the fact of hacking was never conceded, nor was the fact that such hacking had been by Pegasus. At no stage has the father offered any sign of concern for the mother, who is caring for their children, on the basis that her phones have been hacked and her security infiltrated. Instead he has marshalled a formidable forensic team to challenge the findings sought by the mother and to fight the case against her on every point. It is of course the right of a litigant to contest proceedings as they see fit, but to do so may not be without consequences for the relationships of trust and mutual understanding that the court has been keen at all stages to see developing.

## נספח 2

**תגובת המדינה בתיקי האלפים  
לפיה הרוגלה שאבה מידע  
שחרג מצו ביהמ"ש**

עמ' 54

**מדינת ישראל**

באמצעות פרקליטות מחוז תל-אביב (מיסוי וכלכלה)

רחוב מנחם בגין 154, תל אביב 6492107

טלפון: 073-3924600 פקס: 03-5163093

להלן: "המאשימה"

- נ ג ד -

**1. בנימין נתניהו**

באמצעות עו"ד בעז בן צור ואח', מרח' הארבעה

28, תל אביב; טל': 03-7155000; פקס: 03-

7155001; וכן באמצעות עו"ד עמית חדד ואח',

מרחוב וייצמן 2 (בית אמות), תל אביב 6423902;

טל: 03-5333313 פקס: 03-5333314

**2. שאול אלוביץ'**

**3. איריס אלוביץ'**

שניהם באמצעות עו"ד ז'ק חן ואח', מרח' וייצמן

2 (אמות מידה), תל אביב 6423902; טל': 03-

6932077; פקס: 03-6932082

**4. ארנון מוזס**

באמצעות עו"ד נויט נגב, איריס ניב-סבאג ואח',

מרח' וייצמן 2, תל-אביב 6423902; טל': 03-

6099914; פקס: 03-6099915

להלן: "הנאשמים"

**תגובה מטעם המאשימה לבקשות נאשמים 3-1**

בהתאם להחלטת בית המשפט מיום 13.2.2022, מתכבדת המאשימה להגיש תגובתה למספר בקשות שהוגשו מטעם הנאשמים באותו עניין: "בקשה בהולה מטעם נאשמים 2 ו-3" מיום 3.2.2022; "בקשה (דחופה) בעניין שימוש בתוכנה מסוג 'פגסוס'" מטעם נאשם 1 מיום 3.2.2022; ו"בקשה לקבלת חומר חקירה ורשימת חומר שנאסף מתוקנת" מטעם נאשמים 2-3 מיום 10.2.2022 (להלן יחד "בקשות הנאשמים").

בבקשות הנאשמים, שהתבססו על פרסומים עיתונאיים, התבקשו מספר סעדים. ראשית, בית המשפט הנכבד התבקש להורות למאשימה להשיב על שורת שאלות שפורטו בבקשות הנאשמים (סעיף 54 לבקשת נאשם 1, סעיף 14 לבקשת נאשמים 2-3). שנית, בית המשפט הנכבד התבקש להורות, בהתאם לסעיף 74 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982, להעביר לעיון הנאשמים כל חומר חקירה הנוגע לשימוש הנטען בתוכנות רוג'לה במסגרת חקירות הנוגעות לנאשמים. שלישית, בית המשפט הנכבד התבקש להורות למאשימה להמציא רשימה מלאה של החומר שנאסף בתיק, לרבות חומר מודיעין (בקשת נאשמים 2-3 מיום 10.2.2022).

בהחלטתו מיום 13.2.2022 הורה בית המשפט הנכבד למאשימה לכלול בתגובתה לבקשות הנאשמים את "מלוא הפרטים הרלוונטיים, לרבות אופן השימוש בצווים ביחס למי מהנאשמים או העדים".

המאשימה מתכבדת להשיב לבקשות הנאשמים ולהוראת בית המשפט, על סמך בדיקות שערכה משטרת ישראל הן ביחידות החוקרות והן בחטיבת הסייבר-סיגינט, ועל סמך בדיקה שערכה מחלקת חקירות, מודיעין ובקרת מסחר של רשות ניירות ערך, והכל בכפוף לתעודת החיסיון שצומצמה ולדברים שניתן למסור, כדלהלן:

א. מבדיקתה של מחלקת חקירות, מודיעין ובקרת מסחר ברשות ניירות ערך עולה כי לא עשתה מעולם שימוש במערכות טכנולוגיות מסוג "רוגלה", הן בעצמה והן באמצעות משטרת ישראל, וכך גם בתיק זה.

ב. מבדיקתה של משטרת ישראל עולה כי במסגרת חקירת תיק 4000, המשטרה ביקשה וקיבלה צווים שיפוטיים להאזנות סתר לתקשורת בין מחשבים לשני גורמים בתיק: נאשמת 3 והעד שלמה פילבר (להלן: "פילבר"). לצורך מימוש הצווים הללו נעשה שימוש במערכת טכנולוגית (להלן: "המערכת").

ג. הבדיקה מעלה כי משטרת ישראל לא עשתה שימוש במערכת כאמור ביחס לגורמים נוספים שנחקרו בתיק זה בפרשות המכונות "1000" "2000" "4000" וגורמים מפרשות "1270", "1000" הישן, ו-"3H גלובלי".

ד. על פי ממצאי הבדיקה, ביחס לנאשמת 3, הגם שהוצא צו כאמור, לא בוצעה פעולת האזנת הסתר לתקשורת בין מחשבים, חדירה סמויה לחומרי מחשב או כיו"ב, וממילא לא הופק כל תוצר כתוצאה מפעולות אלה.

ה. ביחס לפילבר – הבדיקה העלתה כי הוצא צו, המערכת פעלה על גבי מכשיר הטלפון הסלולרי שלו למשך כיממה (כ-27 שעות), ולא הופקו ממנה תוצרים שהם בגדר "חומר חקירה" הרלוונטי או הנוגע לאישומים. לפיכך, חומר החקירה בתיק אינו כולל חומר כלשהו שהופק באמצעות המערכת.

ו. מבדיקות המשטרה עולה כי במסגרת מימוש הצו האמור בעניינו של פילבר בוצעו פעולות מסוימות, נוסף על האזנות סתר לתקשורת בין מחשבים, במועדים הקבועים בצו, הכוללות גם העתקה של רשימת אנשי הקשר ושל מספר פריטי מידע נוספים שהיו אגורים בטלפון הסלולרי של פילבר (להלן: "הנתונים העודפים").

ז. על פי ממצאי המשטרה, איש היחידה החוקרת שהפיק את האזנות הסתר, המפיק, בחן את תוצרי ההאזנה שנתקבלו כתוצאה מהפעלת המערכת בטווח הזמנים הנקוב בצו הרלוונטי בלבד, ולא עיין בנתונים העודפים שנקלטו על ידי המערכת.

ח. העובדה שבמסגרת מימוש הצו באמצעות המערכת נאספים נתונים עודפים כמפורט בסעיף ו' לעיל לא פורטה בבקשה למתן צו שהוגשה לבית המשפט, ולא הובאה לידיעת ב"כ המאשימה עד למועד הבירור הנוכחי.

ט. צווי האזנות הסתר לתקשורת בין מחשבים בעניינם של נאשמת 3 ושל פילבר נכללו, מלכתחילה, ב"רשימת כל החומר", כדרישת סעיף 74 לחסד"פ, במסגרת החומר המודיעיני שנרשם ברשימת כלל החומר שנאסף. החומרים הללו לא נמסרו לעיון הנאשמים, בהתאם לתעודת החיסיון של המשרד לביטחון פנים, שבה נקבע, כי מטעמים של אינטרס ציבורי חשוב, יש לחסות את עצם קיומם של הצווים ותוצריהם (פריטים אלה מצוינים בסעיף 23 לתעודת החיסיון).

י. נוכח הממצאים שעלו בבדיקת המשטרה כמפורט מעלה, סברה המאשימה כי נכון לצמצם את

היקף החיסיון החל על הצווים. לפיכך, החליט הממונה על החסיונות במשרד לביטחון הפנים, לבקשת המאשימה, לצמצם ולתקן את תעודת החיסיון בתיק, כך שהחיסיון לא יחול עוד על עצם קיום הצווים, ותינתן לנאשמים פרפרזה המתארת את פעולות החקירה שבוצעו לצורך מימוש צו האזנות הסתר. כן הוחלט לתקן את תעודת החיסיון כך שתחול על מזכרים שנערכו על ידי חוקרי משטרה המתארים שיטות ואמצעים של משטרת ישראל, הנוגעים לאופן מימוש הצו, ואשר בשל אינטרס ציבורי חשוב, חסיונם נדרש, בכפוף למסירת הפרפרזה.

יא. המאשימה תמסור לנאשמים רשימה שתכלול פירוט של חומרים נוספים שנוצרו או נאספו במסגרת הבדיקות שנערכו, ובכללם - תעודת החיסיון המעודכנת והפרפרזה המצורפת אליה, החומרים שתעודת החיסיון המעודכנת חלה עליהם, ותרשומות פנימיות בין המאשימה ליחידות החוקרות. יובהר כי תרשומות פנימיות אלה אינן בגדר "חומר חקירה" ולפיכך הן תיכללנה ברשימת החומר שנאסף אך לא תימסרנה לעיון הנאשמים.

### **להלן תובא תגובת המאשימה ביתר פירוט.**

1. בעקבות פרסומים עיתונאיים שבהם נטען שמסגרת ישראל עשתה שימוש נרחב בתוכנות "רוגלה" כחלק מחקירות פליליות שניהלה, פנו ב"כ נאשם 1 למאשימה לראשונה ביום 20.1.2022 בשאלה, אם בוצע שימוש ב"רוגלות" במסגרת חקירות הקשורות לנאשם 1. בפניות נוספות, ביקשו באי כוח הנאשמים לקבל תשובות לשאלות נוספות בנושא זה. עיקרן של שאלות אלו מפורט גם בבקשות הנאשמים שהוגשו לבית המשפט הנכבד.
2. בעקבות פניית הנאשמים והפרסומים העיתונאיים, פנתה המאשימה ליחידות החוקרות וביקשה מהן לבצע בדיקות על מנת לברר את הבסיס העובדתי המדויק והמלא לצורך גיבוש תשובתה לפניות הנאשמים. בהתאם, הודיעה המאשימה מספר פעמים לב"כ הנאשמים, כי נערכת בדיקה מעמיקה של פנייתם. המאשימה אף ביקשה אורכות מבית המשפט הנכבד על מנת ליתן תשובה מלאה ככל הניתן.
3. בעקבות פניית המאשימה, נמסרו לה מן היחידות החוקרות הפרטים הבאים.
4. מחלקת חקירות, מודיעין ובקרת מסחר ברשות ניירות ערך, שניהלה את חקירת התיק המכונה "תיק בזק" במחצית השנייה של שנת 2017, וחקרה במסגרת זו את "פרשה 3" שהתפתחה לימים לחקירת 4000, והיתה שותפה לחקירת תיק 4000 במסגרת צוות חקירה משותף עם משטרת ישראל - הודיעה כי בתיקי החקירה שלה, לרבות בתיק הנוכחי, היא לא עשתה שימוש כלשהו בכלים המכונים "תוכנת רוגלה". זאת, הן בעצמה והן באמצעות פניה לקבלת סיוע ממשטרת ישראל.
5. ממשטרת ישראל נמסר, לאחר בדיקה מול היחידות החוקרות ומול חטיבת הסייבר-סיגינט באגף החקירות והמודיעין, כי השימוש במערכת כאמור נועד לצורך מימושם של צווי האזנות סתר לתקשורת בין מחשבים.
6. בדיקת המשטרה העלתה כי בתיקי החקירה של פרשות 1000 ו-2000 (האישומים השלישי והשני בהתאמה), וכן ביחס לגורמים המעורבים בתיקי החקירה המכונים "1000 הישן", "-1270" ו-"H3גלובל", לא הוצאו צווי האזנת סתר לתקשורת בין מחשבים ולא נעשה שימוש במערכת. בדיקת המשטרה נעשתה מול רשימת המעורבים שסופקה לה על-ידי המאשימה, ומול כלל מספרי הטלפון של מעורבים אלה אשר היו בידיעת המשטרה.
7. בדיקת המשטרה ביחס לתיק 4000 העלתה כי ביום 11.2.2018 הוצאו שני צווי האזנת סתר לתקשורת בין מחשבים, ביחס לפילבר ולנאשמת 3. זאת, לצורך יירוט תקשורת לטווח הזמנים שבין התאריכים 11.2.18-6.3.18. הוצאתם של צווי האזנת סתר לתקשורת בין מחשבים

במסגרת חקירת תיק 4000 לטווח הזמנים שצוין בצווים אושרה על ידי הגורמים המוסמכים בפרקליטות המדינה עובר לפניה לבית המשפט בבקשה למתן הצווים ועל בסיסם. בבקשות לצווי האזנות הסתר הנ"ל נכללה התייחסות לשיטת ההאזנה, לסוגי תוצרים אפשריים שבכוונת המשטרה לקבל, ולפעולות הדרושות להאזנה במסגרת סמכויות העזר. צווי האזנת הסתר ניתנו על ידי נשיא בית משפט מחוזי.

8. בעקבות מתן צווי האזנת הסתר כאמור, ולצורך מימושם, הופעלה המערכת שבשימוש המשטרה. בעניינה של נאשמת 3, ניסיון הפעלת המערכת בעקבות הצו לא צלח, ומשכך, ממילא, לא הניב תוצרים.

9. בעניינו של פילבר, המערכת הופעלה והניבה תוצרים למשך מעט יותר מיממה, מיום 15.2.18 בשעה 12:24 ועד ליום 16.2.18 בשעה 16:55. תוצרים אלה, היינו ההודעות ותיעוד השיחות שנתקבלו כתוצאה מהפעלת המערכת בטווח זמנים זה, נבחנו על ידי מפיק סיגינט מהיחידה החוקרת, שסיווג תוצרים ספורים כרלוונטיים. בתום החקירה סווגו כלל התוצרים על ידי היחידה החוקרת כלא רלוונטיים. הבקשה לחסות את הצווים הללו ותוצריהם, בשלב הוצאת תעודת החיסיון, אושרה לאחר בחינת הפרקליטות.

10. יצוין כי במסגרת הבדיקות שנערכו בתקופה האחרונה הוצגו על ידי נציגי משטרת ישראל לנציגי המאשימה כלל התוצרים שהופקו כתוצאה ממימוש הצו בטווח הזמנים הרלוונטי, ולאחר בחינה נוספת של הדברים דבקה המאשימה בעמדתה כי תוצרים אלה אכן אינם כוללים כל חומר חקירה העשוי להיות רלוונטי או נוגע לתיק.

11. בצד הפקת התוצרים בהתאם לצו, ביצעה המערכת פעולות מסוימות נוסף על האזנת סתר לתקשורת בין מחשבים, הכוללות גם העתקה של רשימת אנשי הקשר והעתקה של מספר פריטי מידע נוספים שהיו אגורים בטלפון הסלולרי של פילבר. פרטים אלה לא פורטו במפורש בבקשה למתן צו שהוגשה לבית המשפט, ולא הובאו לידיעת ב"כ המאשימה בעת אישור הבקשה לצווים על ידי גורמי הפרקליטות או מאוחר יותר, בעת אישור הבקשה לחסיונם.

12. הנתונים העודפים שמורים במסד הנתונים של המערכת שמצויה היתה ביחידה משטרתית שאינה היחידה החוקרת. מפיק האזנות הסתר לא עיין בהם והם אף לא הועברו לעיון היחידה החוקרת.

13. במסגרת תעודת החיסיון שהוצאה בתיק נחסה עצם קיומם של צווי האזנת הסתר לתקשורת בין מחשבים, פעולות החקירה המתועדות בהם ותוצריהם, וזאת מטעמים של אינטרס ציבורי חשוב. החומרים שנחסו נרשמו ב"רשימת כל החומר", שנמסרה לעיון הנאשמים (שורות 2035 בלשונית סימון מסמכים 4000).

14. במסגרת הבדיקות שנתבקשה לערוך משטרת ישראל, כמצוין לעיל בסעיף 2, ובצד הממצאים שפורטו לעיל, ביצעה המשטרה בדיקה מקיפה יותר של כלל הגורמים שנחקרו בתיקי החקירה הנוגעים לתיק שבכותרת (תיקי החקירה הידועים כ"תיק 1000", "תיק 2000", "תיק 4000"). כמו כן נבדקו גורמים נוספים מתוך תיקי החקירה 1270 ותיק המכונה "1000 הישן". הבדיקות בוצעו הן ביחס לקיומם של צווים מתאימים והן ביחס למספרי טלפון המשויכים לגורמים שנבדקו במערכות המשטרה השונות. בדיקות אלה נערכו במערכות המשטרה ובשלב מסוים נעשתה אף בדיקה מצליבה משלימה של נתונים מסוימים מול בסיס נתונים של המערכת של שרת חברת NSO הנמצא בחוות-השרתים של משטרת-ישראל, והונגש לגורמים במשטרת-ישראל באמצעות נציגי חברת NSO. בדיקה זו הושלמה אתמול ביום 15.2.22 ולא העלתה ממצאים נוספים כלשהם מעבר למפורט במסמך זה.

15. במסגרת זו נבדק אם הוצאו או התבקשו צווי האזנת סתר בנוגע למי מהגורמים הנ"ל, מעבר לצווים המצויים בחומרי החקירה; כמו כן, נבדק אם הופעלה המערכת הטכנולוגית, או כל מערכת טכנולוגית אחרת בעלת מאפיינים דומים שבשימוש המשטרה, מול מספרי הטלפון השייכים לכל אותם גורמים. הבדיקה נערכה ביחס לכ-1500 מספרי טלפון המשוויכים לכ-225 מעורבים בתיקים אלה.

**כפי שנמסר למאשימה על ידי משטרת ישראל, ממצאי בדיקתה המקיפה מעלים שהמערכת, או כל מערכת טכנולוגית אחרת בעלת מאפיינים דומים שבשימוש המשטרה, לא הופעלה לגבי הגורמים שנבדקו במסגרת תיקי החקירה האמורים, למעט ביחס לפילבר ולנאשמת 3, שלגביהם כאמור הוצאו צווי האזנת סתר לתקשורת בין מחשבים.**

מעבר לנדרש יצוין, כי הבדיקה העלתה שביחס לאחד העדים בתיק, הוצא צו האזנת סתר לתקשורת בין מחשבים במסגרת תיק חקירה אחר בו היה חשוד. הצו לא מומש וממילא לא בוצע בעניינו כל שימוש במערכת או בכל מערכת טכנולוגית אחרת בעלת מאפיינים דומים שבשימוש המשטרה. משכך אין במידע האמור כל רלוונטיות לתיק זה, והדברים הובאו מעבר לנדרש לצורך מתן מידע מלא על תוצאות הבדיקה בלבד.

16. נוכח ממצאים אלה של משטרת ישראל סברה המאשימה, כי נכון לחשוף בפני הנאשמים את עובדת קליטתם של נתונים עודפים במסגרת פעולת המערכת לצורך מימוש הצו בעניינו של פילבר. לצד זאת יש עדיין אינטרס ציבורי חשוב בחיסיון על שיטות ואמצעים של משטרת ישראל. לפיכך, פנתה המאשימה לממונה על החסיונות בבקשה לצמצם ולעדכן את תעודת החיסיון בתיק, כך שיוסר החיסיון על עצם קיומם של צווי האזנות הסתר לתקשורת בין מחשבים, זאת, בכפוף למתן פרפרזה על ידי הגורמים המוסמכים במשטרת ישראל, המתארת את הצווים שהוצאו והפעולות שבוצעו לצורך מימושם. בנוסף, נתבקש הממונה על החסיונות להטיל חיסיון על מזכרים המפרטים את פעולות הבדיקה שבוצעו כעת, ושיש בגילויים כדי לפגוע באמצעים ושיטות של היחידות החוקרות, ולסכל פעולות אכיפה עתידיות. היום, 16.2.22, הוציא הממונה על החסיונות תעודת חיסיון מעודכנת בתיק, שהועברה לעיון הנאשמים, ובצידה הפרפרזה האמורה.

17. נוכח האמור, תעביר המאשימה לנאשמים רשימה מעודכנת של החומר שנאסף בתיק, הכוללת ציון של הפריטים הנוספים שתעודת החיסיון המעודכנת חלה עליהם, וכן ציון של תרשומות פנימיות בין המאשימה ליחידות החוקרות, שנערכו לצורך הבדיקה. תרשומות אלה אינן בגדר "חומר חקירה" ולפיכך הן לא נמסרו לעיון הנאשמים. לעמדת המאשימה, בכך היא עומדת בחובותיה לפי סעיף 74 לחסד"פ, נוכח העובדה שהפריטים שחסו תחת תעודת החיסיון המקורית (הצווים ותוצריהם) היו מנויים כבר ב"רשימת כל החומר" שנמסרה לנאשמים בעבר.

18. לאחר הגשת בקשות הנאשמים, במהלך דיון בבית המשפט ובפניה לב"כ המאשימה, הוסיפו הנאשמים וטענו, כי הבדיקות הנוגעות לבקשותיהם צריכות להתבצע באמצעות פניה לחברה המייצרת את המערכת. המאשימה דוחה עמדה זו מכל וכל. על דרך הכלל, טענות הנטענות ביחס להתנהלות רשות חקירה במהלך חקירה מופנות על ידי המאשימה לאותה רשות חקירה לצורך קבלת עמדתה ובדיקותיה. משטרת ישראל אינה הופכת להיות "חשודה", קל וחומר "פסולה" בשל טענות שכאלה. בעניין דנן, כפי שפורט, התבקשה המשטרה וערכה בחינה מעמיקה, יסודית ומקפת על ידי גורמי המטה במשטרה יחד עם היחידות החוקרות – בחינה, שכללה בדיקה במערכות הטכנולוגיות, ולא נמצא כל בסיס להטיל דופי במהימנותה. כתוצאה מן הבחינה היסודית אף אותרו התוצאות שפורטו לעיל, וגם בכך יש כדי ללמד על עומק ומהימנות הבדיקה.

למעלה מן הנדרש כפי שפורט לעיל, חלק מן הבדיקות שערכה משטרת ישראל בוצעו גם בשרתים נוספים שהונגשו על ידי נציגי חברת NSO.

19. למען שלמות התמונה, וללא קשר לפניות הנאשמים בתיק ספציפי זה, תציין המאשימה, כי בהתאם להחלטת היועץ המשפטי לממשלה, מבוצעת בדיקה נפרדת על ידי צוות בראשות המשנה ליועצת המשפטית לממשלה, בסיוע מומחים טכנולוגיים, ובכלל זה ביחס ל-26 גורמים ששמן עליה בפרסומים העיתונאיים, ושחלקם מצוי גם ברשימת הגורמים שנבדקה על ידי משטרת ישראל בתיק שלפנינו, כאמור לעיל. כפי שנמסר לנו, צוות זה טרם השלים את בדיקותיו.

20. מטבע הדברים, ככל שיתגלו ממצאים כלשהם הנוגעים לתיק זה, הדבר יובא בפני המאשימה באופן מיידי, וכל תוכן רלוונטי יימסר להגנה בהתאם לדין.

21. **לסיכום, מבדיקתה היסודית של משטרת ישראל, בהכוונתה של המאשימה, עולה כי, בניגוד לנטען, בתיק שלפנינו נעשה שימוש מצומצם ביותר במערכת טכנולוגית לצורך מימוש צווים שיפוטיים להאזנת סתר לתקשורת בין מחשבים. הלכה למעשה הושגו תוצרים באמצעות המערכת ביחס לגורם אחד בלבד, בתקופת זמן קצרה מאד. השימוש בתוכנה נעשה לאחר הוצאת צו שנחתם על ידי נשיא בית משפט מחוזי. הגם שלצורך מימוש הצו נאגרו נתונים עודפים, הרי שהתוצרים שהופקו כתוצאה מהפעולה שביצעה המערכת נמצאו כלא רלוונטיים, לא הופק מהם כל "חומר חקירה" וממילא לא נעשה בתוצרים כל שימוש במסגרת החקירה.**

22. **נוכח ממצאי בדיקת המשטרה וכל שהובא בתגובה זאת לעיל, ובמיוחד נוכח העובדה שממצאי הבדיקה העלו שאין חומר חקירה רלוונטי שאותר באמצעות המערכת, תטען המאשימה שנכון וראוי להמשיך את שמיעת ההוכחות בתיק שבכותרת כסדרה, ואין כל עילה לדחות את המשך המשפט.**

  
ד"ר אלון גילדין, עו"ד  
מנהל מחלקה  
בפרקליטות מחוז ת"א  
(מיסוי וכלכלה)

  
יהודית תירוש, עו"ד  
מנהלת מחלקת ניירות ערך  
פרקליטות מחוז ת"א  
(מיסוי וכלכלה)

  
ליאת בן-ארי שווקי  
משנה לפרקליט המדינה  
(אכיפה כלכלית)

16 פברואר 2022

ט"ו אדר א תשפ"ב

### נספח 3

## **מסמך מיחידת הסיגינט במשטרה**

עמ' 61

57

- סודי ביותר -

האגף לחקירות ולמודיעין  
חטיבת הסייבר  
טלפון: 02-5427121  
פקס: 02-5427140  
27 בינואר 2022



ד"ר חיים ויסמונסקי/ראש מחלקת הסייבר- פרקליטות המדינה

**הנדון: הבהרות בנוגע לתוצרי הא"ס בתיק**

הבהרה: הנתונים המפורטים במסמך הנ"ל הינם לטובת הבהרות טכנולוגיות הנדרשות לפרקליטות המדינה ואינם חלק מחומר החקירה. יש לשמור על רגישות המסמך ואין להעבירו לגורם בלתי מורשה.

1. בפרשייה של לחב 433/יאלי"כ הופעלו יכולות הא"ס מתקדמות על יעד ש.פ.
2. צו הא"ס הוצא לתקופה 11.2.2018-6.3.2018.
3. במסמך יוסברו נתונים שהתקבלו במסגרת יכולות הא"ס של המערכת ביעד ש.פ., והגדרת החומרים שהופקו בתיק.
4. הבהרה: לא מבוצעות פעולות הא"ס במערכת לפני קבלת צו הא"ס ואישורו.
5. ככלל, לא נאספים נתונים שאינם במסגרת חלון הזמנים המותר בצו, או סוגי מידע שאינם תוצרי הא"ס, מלבד נתונים הנדרשים כפי שיפורט בהמשך.
6. בנוסף, ישנם סוגי מידע שאינם מוגדרים כתוצרי הא"ס ויכולים להתקבל (כפי שיפורט לחלוף), על אף שתוצרים אלו נגשים למפיק, אינם אמורים להיות מנותחים ומופקים על ידו.
7. נתונים שהתקבלו ביעד ש.פ.:

אנשי קשר - במועד הטיפול בתיק נתונים אלו מתקבלים אוטומטית

[Redacted text block]

נתונים נלווים הנדרשים

[Redacted text block]

[Redacted text block]

[Redacted text block]

בברכה,

חטיבת הסייבר

**נספח 4**

**פרסום בניו יורקר של רונן פארו**

**עמ' 63**

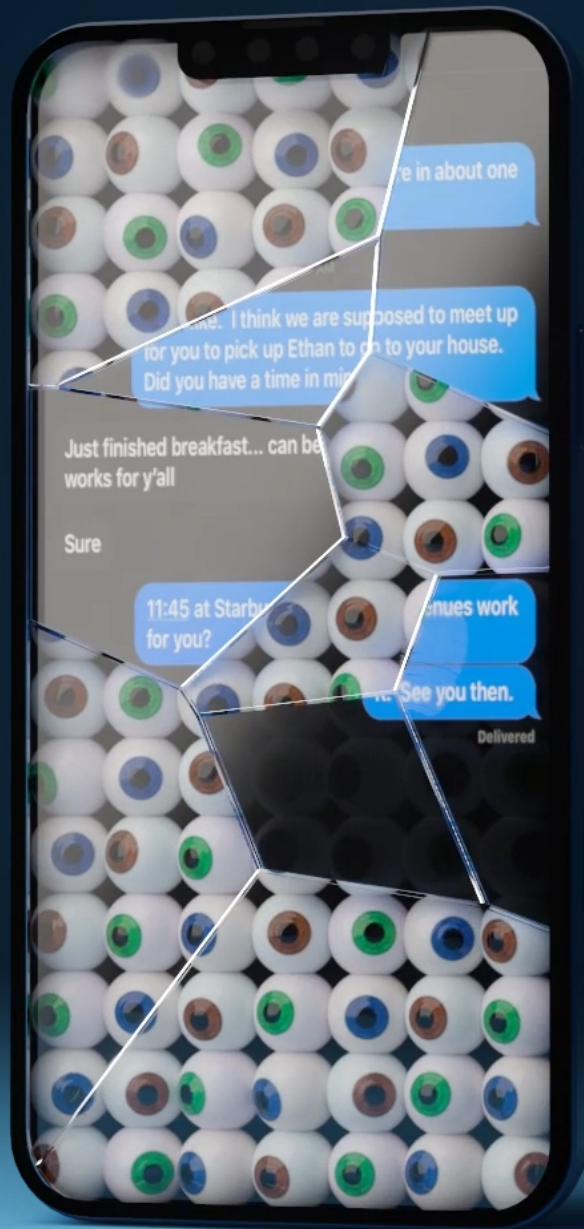
A REPORTER AT LARGE APRIL 25 & MAY 2, 2022 ISSUE

# HOW DEMOCRACIES SPY ON THEIR CITIZENS

*The inside story of the world's most notorious commercial spyware and the big tech companies waging war against it.*

**By Ronan Farrow**

April 18, 2022



*NSO Group's software has been linked to repressive regimes, but now "all types of governments" use it, an observer said.* Illustration by Timo Lenzen

☐ Listen to this story



0:00 / 57:03

To hear more, download the Audm app.

The parliament of Catalonia, the autonomous region in Spain, sits on the edge of Barcelona's Old City, in the remains of a fortified citadel constructed by King Philip V to monitor the restive local population. The citadel was built with forced labor from hundreds of Catalans, and its remaining structures and gardens are for many a reminder of oppression. Today, a majority of Catalan parliamentarians support independence for the region, which the Spanish government has deemed

unconstitutional. In 2017, as Catalonia prepared for a referendum on independence, Spanish police arrested at least twelve separatist politicians. On the day of the referendum, which received the support of ninety per cent of voters despite low turnout, police raids of polling stations injured hundreds of civilians. Leaders of the independence movement, some of whom live in exile across Europe, now meet in private and communicate through encrypted messaging platforms.

One afternoon last month, Jordi Solé, a pro-independence member of the European Parliament, met a digital-security researcher, Elies Campo, in one of the Catalan parliament's ornate chambers. Solé, who is forty-five and wore a loose-fitting suit, handed over his cell phone, a silver iPhone 8 Plus. He had been getting suspicious texts and wanted to have the device analyzed. Campo, a soft-spoken thirty-eight-year-old with tousled dark hair, was born and raised in Catalonia and supports independence. He spent years working for WhatsApp and Telegram in San Francisco, but recently moved home. "I feel in a way it's a kind of duty," Campo told me. He now works as a fellow at the Citizen Lab, a research group based at the University of Toronto that focusses on high-tech human-rights abuses.

Campo collected records of Solé's phone's activity, including crashes it had experienced, then ran specialized software to search for spyware designed to operate invisibly. As they waited, Campo looked through the phone for evidence of attacks that take varied forms: some arrive through WhatsApp or as S.M.S. messages that seem to come from known contacts; some require a click on a link, and others operate with no action from the user. Campo identified an apparent notification from the Spanish government's social-security agency which used the same format as links to malware that the Citizen Lab had found on other phones. "With this message, we have the proof that at some point you were attacked," Campo explained. Soon, Solé's phone vibrated. "This phone tested positive," the screen read. Campo told Solé, "There's two confirmed infections," from June, 2020. "In those days, your device was infected—they took control of it and were on it probably for some hours. Downloading, listening, recording."

Solé's phone had been infected with Pegasus, a spyware technology designed by NSO Group, an Israeli firm, which can extract the contents of a phone, giving access to its texts and photographs, or activate its camera and microphone to provide real-time surveillance—exposing, say, confidential meetings. Pegasus is useful for law enforcement seeking criminals, or for authoritarians looking to quash dissent. Solé had been hacked in the weeks before he joined the European Parliament, replacing a colleague who had been imprisoned for pro-independence activities. "There's been a clear political and judicial persecution of people and elected representatives," Solé told me, "by using these dirty things, these dirty methodologies."

In Catalonia, more than sixty phones—owned by Catalan politicians, lawyers, and activists in Spain and across Europe—have been targeted using Pegasus. This is the largest forensically documented cluster of such attacks and infections on record. Among the victims are three members of the European Parliament, including Solé. Catalan politicians believe that the likely perpetrators of the hacking campaign are Spanish officials, and the Citizen Lab's analysis suggests that the Spanish government has used Pegasus. A former NSO employee confirmed that the company has an account in Spain. (Government agencies did not respond to requests for comment.) The results of the Citizen Lab's investigation are being disclosed for the first time in this article. I spoke with more than forty of the targeted individuals, and the

conversations revealed an atmosphere of paranoia and mistrust. Solé said, “That kind of surveillance in democratic countries and democratic states—I mean, it’s unbelievable.”

[*Support The New Yorker’s award-winning journalism. [Subscribe today](#)»*]

Commercial spyware has grown into an industry estimated to be worth twelve billion dollars. It is largely unregulated and increasingly controversial. In recent years, investigations by the Citizen Lab and Amnesty International have revealed the presence of Pegasus on the phones of politicians, activists, and dissidents under repressive regimes. An analysis by Forensic Architecture, a research group at the University of London, has linked Pegasus to three hundred acts of physical violence. It has been used to target members of Rwanda’s opposition party and journalists exposing corruption in El Salvador. In Mexico, it appeared on the phones of several people close to the reporter Javier Valdez Cárdenas, who was murdered after investigating drug cartels. Around the time that Prince Mohammed bin Salman of Saudi Arabia approved the murder of the journalist Jamal Khashoggi, a longtime critic, Pegasus was allegedly used to monitor phones belonging to Khashoggi’s associates, possibly facilitating the killing, in 2018. (Bin Salman has denied involvement, and NSO said, in a statement, “Our technology was not associated in any way with the heinous murder.”) Further reporting through a collaboration of news outlets known as the Pegasus Project has reinforced the links between NSO Group and anti-democratic states. But there is evidence that Pegasus is being used in at least forty-five countries, and it and similar tools have been purchased by law-enforcement agencies in the United States and across Europe. Cristin Flynn Goodwin, a Microsoft executive who has led the company’s efforts to fight spyware, told me, “The big, dirty secret is that governments are buying this stuff—not just authoritarian governments but all types of governments.”

NSO Group is perhaps the most successful, controversial, and influential firm in a generation of Israeli startups that have made the country the center of the spyware industry. I first interviewed Shalev Hulio, NSO Group’s C.E.O., in 2019, and since then I have had access to NSO Group’s staff, offices, and technology. The company is in a state of contradiction and crisis. Its programmers speak with pride about the use of their software in criminal investigations—NSO claims that Pegasus is sold only to law-enforcement and intelligence agencies—but also of the illicit thrill of compromising technology platforms. The company has been valued at more than a billion dollars. But now it is contending with debt, battling an array of corporate backers, and, according to industry observers, faltering in its long-standing efforts to sell its products to U.S. law enforcement, in part through an American branch, Westbridge Technologies. It also faces numerous lawsuits in many countries, brought by Meta (formerly Facebook), by Apple, and by individuals who have been hacked by NSO. The company said in its statement that it had been “targeted by a number of politically motivated advocacy organizations, many with well-known anti-Israel biases,” and added that “we have repeatedly cooperated with governmental investigations, where credible allegations merit, and have learned from each of these findings and reports, and improved the safeguards in our technologies.” Hulio told me, “I never imagined in my life that this company would be so famous. . . . I never imagined that we would be so successful.” He paused. “And I never imagined that it would be so controversial.”

**H**ulio, who is forty, has a lumbering gait and pudgy features. He typically wears loose T-shirts and jeans, with his hair in a utilitarian buzz cut. Last month, I visited him at his duplex in a luxury high-rise in Park Tzameret, the fanciest neighborhood in Tel Aviv. He lives with his three small children

and his wife, Avital, who is expecting a fourth. There's a pool on the upper level of Hulio's apartment, and downstairs, in the double-height living room, is a custom arcade cabinet stocked with retro games and bearing a cartoon portrait of him, wearing shades, next to the word "Hulio" in large eight-bit font. Avital attends to the children, frequent renovations, and an ever-shifting array of pets: rabbits remain, a parrot does not. The family has a teacup poodle named Marshmallow Rainbow Sprinkle.

Hulio, Omri Lavie, and Niv Karmi founded NSO Group in 2010, creating its name from the first letters of their names and renting space in a converted chicken coop on a kibbutz. The company now has some eight hundred employees, and its technology has become a leading tool of state-sponsored hacking, instrumental in the fight among great powers.



m.e. mcnair

*"Your résumé looks terrific, but I'm just not sure we can deal with the shedding."*



Cartoon by Elisabeth McNair

The Citizen Lab's researchers concluded that, on July 26 and 27, 2020, Pegasus was used to infect a device connected to the network at 10 Downing Street, the office of Boris Johnson, the Prime Minister of the United Kingdom. A government official confirmed to me that the network was compromised, without specifying the spyware used. "When we found the No. 10 case, my jaw dropped," John Scott-

Railton, a senior researcher at the Citizen Lab, recalled. “We suspect this included the exfiltration of data,” Bill Marczak, another senior researcher there, added. The official told me that the National Cyber Security Centre, a branch of British intelligence, tested several phones at Downing Street, including Johnson’s. It was difficult to conduct a thorough search of phones—“It’s a bloody hard job,” the official said—and the agency was unable to locate the infected device. The nature of any data that may have been taken was never determined.

The Citizen Lab suspects, based on the servers to which the data were transmitted, that the United Arab Emirates was likely behind the hack. “I’d thought that the U.S., U.K., and other top-tier cyber powers were moving slowly on Pegasus because it wasn’t a direct threat to their national security,” Scott-Railton said. “I realized I was mistaken: even the U.K. was underestimating the threat from Pegasus, and had just been spectacularly burned.” The U.A.E. did not respond to multiple requests for comment, and NSO employees told me that the company was unaware of the hack. One of them said, “We hear about every, every phone call that is being hacked over the globe, we get a report immediately”—a statement that contradicts the company’s frequent arguments that it has little insight into its customers’ activities. In its statement, the company added, “Information raised in the inquiry indicates that these allegations are, yet again, false and could not be related to NSO products for technological and contractual reasons.”

According to an analysis by the Citizen Lab, phones connected to the Foreign Office were hacked using Pegasus on at least five occasions, from July, 2020, through June, 2021. The government official confirmed that indications of hacking had been uncovered. According to the Citizen Lab, the destination servers suggested that the attacks were initiated by states including the U.A.E., India, and Cyprus. (Officials in India and Cyprus did not respond to requests for comment.) About a year after the Downing Street hack, a British court revealed that the U.A.E. had used Pegasus to spy on Princess Haya, the ex-wife of Sheikh Mohammed bin Rashid al-Maktoum, the ruler of Dubai, one of the Emirates. Maktoum was engaged in a custody dispute with Haya, who had fled with their two children to the U.K. Her attorneys, who are British, were also targeted. A source directly involved told me that a whistle-blower contacted NSO to alert it to the cyberattack on Haya. The company enlisted Cherie Blair, the wife of former Prime Minister Tony Blair and an adviser to NSO, to notify Haya’s attorneys. “We alerted everyone in time,” Hulio told me. Soon afterward, the U.A.E. shut down its Pegasus system, and NSO announced that it would prevent its software from targeting U.K. phone numbers, as it has long done for U.S. numbers.

Elsewhere in Europe, Pegasus has filled a need for law-enforcement agencies that previously had limited cyber-intelligence capacity. “Almost all governments in Europe are using our tools,” Hulio told me. A former senior Israeli intelligence official added, “NSO has a monopoly in Europe.” German, Polish, and Hungarian authorities have admitted to using Pegasus. Belgian law enforcement uses it, too, though it won’t admit it. (A spokesperson for the Belgian federal police said that it respects “a legal framework as to the use of intrusive methods in private life.”) A senior European law-enforcement official whose agency uses Pegasus said that it gave an inside look at criminal organizations: “When do they want to store the gas, to go to the place, to put the explosive?” He said that his agency uses Pegasus only as a last resort, with court approval, but conceded, “It’s like a weapon. . . . It can always occur that an individual uses it in the wrong way.”

The United States has been both a consumer and a victim of this technology. Although the National Security Agency and the C.I.A. have their own surveillance technology, other government offices, including in the military and in the Department of Justice, have bought spyware from private companies, according to people involved in those transactions. The *Times* has reported that the F.B.I. purchased and tested a Pegasus system in 2019, but the agency denied deploying the technology.

Establishing strict rules about who can use commercial spyware is complicated by the fact that such technology is offered as a tool of diplomacy. The results can be chaotic. The *Times* has reported that the C.I.A. paid for Djibouti to acquire Pegasus, as a way to fight terrorism. According to a previously unreported investigation by WhatsApp, the technology was also used against members of Djibouti's own government, including its Prime Minister, Abdoukadar Kamil Mohamed, and its Minister of the Interior, Hassan Omar.

Last year, as the *Washington Post* reported and Apple disclosed in a legal filing, the iPhones of eleven people working for the U.S. government abroad, many of them at its embassy in Uganda, were hacked using Pegasus. NSO Group said that, "following a media inquiry" about the incident, the company "immediately shut down all the customers potentially relevant to this case, due to the severity of the allegations, and even before we began the investigation." The Biden Administration is investigating additional targeting of U.S. officials, and has launched a review of the threats posed by foreign commercial hacking tools. Administration officials told me that they now plan to take new, aggressive steps. The most significant is "a ban on U.S. government purchase or use of foreign commercial spyware that poses counterintelligence and security risks for the U.S. government or has been improperly used abroad," Adrienne Watson, a White House spokesperson, said.

In November, the Commerce Department added NSO Group, along with several other spyware makers, to a list of entities blocked from purchasing technology from American companies without a license.

I was with Hulio in New York the next day. NSO could no longer legally buy Windows operating systems, iPhones, Amazon cloud servers—the kinds of products it uses to run its business and build its spyware. "It's outrageous," he told me. "We never sold to any country which is not an ally with the U.S., or an ally of Israel. We've never sold to any country the U.S. doesn't do business with." Deals with foreign clients require "direct written approval from the government of Israel," Hulio said.

"I think that it is not well understood by American leaders," Eva Galperin, the director of cybersecurity at the watchdog group Electronic Frontier Foundation, told me. "They keep expecting that the Israeli government will crack down on NSO for this, whereas, in fact, they're doing the Israeli government's bidding." Last month, the *Washington Post* reported that Israel had blocked Ukraine from purchasing Pegasus, not wanting to alienate Russia. "Everything that we are doing, we got the permission from the government of Israel," Hulio told me. "The entire mechanism of regulation in Israel was built by the Americans."

NSO sees itself as a type of arms dealer, operating in a field without established norms. Hulio said, "There is the Geneva Conventions for the use of a weapon. I truly believe that there should be a convention of countries that should agree between themselves on the proper use of such tools" for cyber warfare. In the absence of international regulation, a battle is taking place between private companies: on

one side, firms like NSO; on the other, the major technology platforms through which such firms implement their spyware.

On Thursday, May 2, 2019, Claudiu Dan Gheorghe, a software engineer, was working at Building 10 on Facebook's campus in Menlo Park, where he managed a team of seven people responsible for WhatsApp's voice- and video-calling infrastructure. Gheorghe, who was born in Romania, is thirty-five, with a slight frame and dark, close-cropped hair. In a photograph he used as a professional head shot during his nine years at Facebook, he wears a black hoodie and looks a little like Elliot Alderson, the protagonist of the hacking drama "Mr. Robot." Building 10 is a two-story structure with open-plan workspaces, brightly colored accent walls, and whiteboards. Engineers, most of them in their twenties and thirties, hunch over keyboards. The word "focus" is written on a wall and stamped on magnets scattered around the office. "It often felt like a church," Gheorghe recalled. WhatsApp, which Facebook bought for nineteen billion dollars in 2014, is the world's most popular messaging application, with about two billion monthly users.

Facebook had presented the platform, which uses end-to-end encryption, as ideal for sensitive communications; now the company's security team was more than two years into an effort to reinforce the security of its products. One task entailed looking at "signalling messages" automatically sent by WhatsApp users to the company's servers, in order to initiate calls. That evening, Gheorghe was alerted to an unusual signalling message. A piece of code that was intended to dictate the ringtone contained, instead, code with strange instructions for the recipient's phone.

In a system as vast as Facebook's, anomalies were routine, and usually innocuous. Unfamiliar code can stem from an older version of the software, or it can be a stress test by Facebook's Red Team, which conducts simulated attacks. But, as engineers in Facebook's international offices awoke and began to scrutinize the code, they grew concerned. Otto Ebeling, who worked on Facebook's security team in London, told me that the code seemed "polished, slick, which was alarming." Early on the morning after the message was discovered, Joaquin Moreno Garijo, another member of the London security team, wrote on the company's internal messaging system that, owing to how sophisticated the code was, "we believe that attacker may have found a vulnerability." Programmers who work on security issues often describe their work in terms of vulnerabilities and exploits. Ivan Krstić, an engineer at Apple, compared the concept to a heist scene in the film "Ocean's Twelve," in which a character dances through a hall filled with lasers that trigger alarms. "In that scene, the vulnerability is that there exists a path through all the lasers, where it's possible to get across the room," Krstić said. "But the exploit is that somebody had to be a precise enough dancer to actually be able to do that dance."

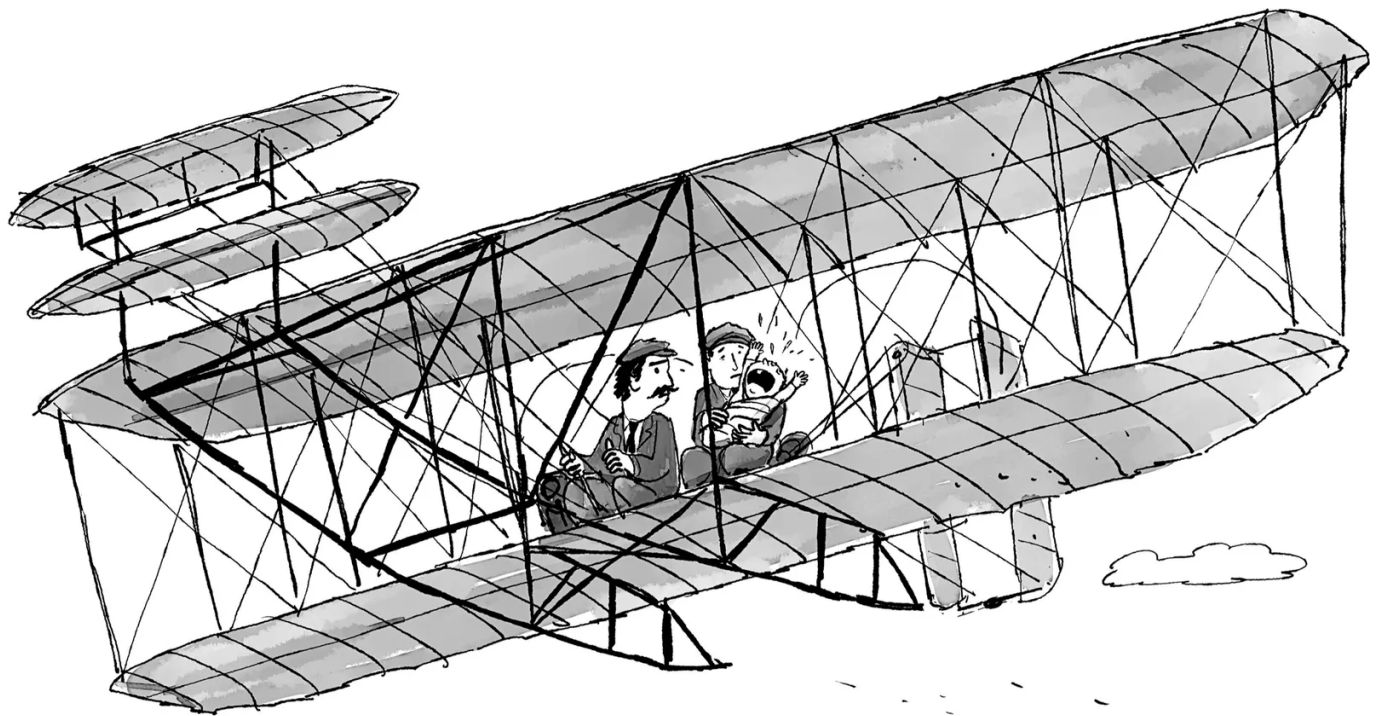
By late Sunday, a group of engineers working on the problem had become convinced that the code was an active exploit, one that was attacking vulnerabilities in their infrastructure as they watched. They could see that data were being copied from users' phones. "It was scary," Gheorghe recalled. "Like the world is sort of shaking under you, because you built this thing, and it's used by so many people, but it has this massive flaw in it."

The engineers quickly identified ways to block the offending code, but they debated whether to do so. Blocking access would tip off the attackers, and perhaps allow them to erase their tracks before the engineers could make sure that any solution closed all possible avenues of attack. "That would be like chasing ghosts," Ebeling said. "Made a decision to not roll out the server-side fix," Andrey Labunets, a

WhatsApp security engineer, wrote, in an internal message, “because we don’t understand the root cause the impact for users and other possible attacker numbers / techniques.”

On Monday, at crisis meetings with WhatsApp’s top executive, Will Cathcart, and Facebook’s head of security, the company told its engineers around the world that they had forty-eight hours to investigate the problem. “What would the scale of the victims be?” Cathcart recalled worrying. “I mean, how many people were hit by this?” The company’s leadership decided not to notify law enforcement immediately, fearing that U.S. officials might tip off the hackers. “There’s a risk of—you might go to someone who’s a customer,” he told me. (Their concerns were valid: weeks later, the *Times* has reported, the F.B.I. hosted NSO engineers at a facility in New Jersey, where the agency tested the Pegasus software it had purchased.) Cathcart alerted Mark Zuckerberg, who considered the problem “horrific,” Cathcart recalled, and pressed the team to work quickly. For Gheorghe, “it was a terrifying Monday. I woke up at like 6 A.M., and then I worked until I couldn’t stay awake anymore.”

NSO’s headquarters are in a glass-and-steel office building in Herzliya, a suburb outside Tel Aviv. The area is home to a cluster of technology firms from Israel’s thriving startup sector. The beach is a twenty-minute walk away. The world’s most notorious commercial hacking enterprise is remarkably unprotected: at times, a single security guard waved me through.



THE WRIGHT BROTHERS DISCOVER THE FIRST NIGHTMARE FLIGHT

On the building's fourteenth floor, programmers wearing hoodies gather in a cafeteria outfitted with an espresso machine and an orange juicer, or sit on a terrace with views of the Mediterranean. A poster reads "LIFE WAS MUCH EASIER WHEN APPLE AND BLACKBERRY WERE JUST FRUITS." Stairs descend to the various programming groups, each of which has its own recreational space, with couches and PlayStation 5s. The Pegasus team likes to play Electronic Arts' football game, FIFA.

Employees told me that the company keeps its technology covert through an information-security department with several dozen experts. "There is a very large department in the company which is in charge of whitewashing, I would say, all connection, all network connection between the client back to NSO," a former employee said. "They are purchasing servers, V.P.N. servers around the world. They have, like, this whole infrastructure set up so none of the communication can be traced."

Despite these precautions, WhatsApp engineers managed to trace data from the hack to I.P. addresses tied to properties and Web services used by NSO. "We now knew that one of the biggest threat actors in the world has a live exploit against WhatsApp," Gheorghe recalled. "I mean, it was exciting, because it's very rare to catch some of these things. But, at the same time, it was also extremely scary." A picture of the victims began to emerge. "Likely there are journalists human rights activists and others on the list," Labunets, the security engineer, wrote on the company's messaging system. (Eventually, the team identified some fourteen hundred WhatsApp users who had been targeted.)

By midweek, about thirty people were working on the problem, operating in a twenty-four-hour relay, with one group going to sleep as another came online. Facebook extended the team's deadline, and they began to reverse engineer the malicious code. "To be honest, it's brilliant. I mean, when you look at it, it feels like magic," Gheorghe said. "These people are very smart," he added. "I don't agree with what they do, but, man, that is a very complicated thing they built." The exploit triggered two video calls in close succession, one joining the other, with the malicious code hidden in their settings. The process took only a few seconds, and deleted any notifications immediately afterward. The code used a technique known as a "buffer overflow," in which an area of memory on a device is overloaded with more data than it can accommodate. "It's like you're writing on a piece of paper and you go beyond the bounds," Gheorghe explained. "You start writing on whatever the surface is, right? You start writing on the desk." The overflow allows the software to overwrite surrounding sections of memory freely. "You can make it do whatever you want."

I spoke with a vice-president for product development at NSO, whom the firm requested I identify only by his first name, Omer—citing, without apparent irony, privacy concerns. "You find the nooks and crannies enabling you to do something that the product designer didn't intend," Omer told me. Once in control, the exploit loaded more software, allowing the attacker to extract data or activate a camera or a microphone. The entire process was "zero click," requiring no action from the phone's owner.

The software was designed by NSO's Core Research Group, made up of several dozen software developers. "You're looking for a silver bullet, a simple exploit that can cover as much mobile devices around the world," Omer told me. Gheorghe said, "A lot of people, you know, would think about the hackers as being, like, just one person in a dark room, like, typing on a keyboard, right? That's not the

reality—these people are just, like, another tech company.” It is common for tech companies to hire people with backgrounds in hacking, and to offer bounties to outside programmers who identify vulnerabilities in their systems. Facebook’s headquarters have the vanity address 1 Hacker Way. At both NSO and WhatsApp, the engineers closest to the coding are often described by colleagues as quirky introverts, resembling the hacker archetypes of fiction. “They are special people. Not all of them can communicate clearly with other human beings,” Omer said, of the programmers who work on Pegasus. “Some of them don’t sleep for two days. They get crazy when they don’t sleep.”

Late in the week, Facebook’s security team devised an act of subterfuge: they would simulate an infected device, to get NSO’s servers to send them a copy of the code. “But their software was smart enough to basically not be tricked by this,” Gheorghe said. “We never really were able to get our hands on that.”

Omer told me, “It’s a cat-and-mouse game.” Although NSO says that its customers control the use of Pegasus, it does not dispute its direct role in these exchanges. “Every day, things are being patched,” Hulio said. “This is the routine work here.”

At times, WhatsApp users received repeated missed calls, but the malware wasn’t successfully installed. Once the engineers learned about these incidents, they were able to study what it looked like when Pegasus failed. Toward the end of the week, Gheorghe told me, “we said, O.K., we don’t have a full understanding at this point, but I think we captured enough.” On Friday morning, Facebook notified the Department of Justice, which is developing a case against NSO. Then the company updated its servers to block the malicious code. “Ready to roll,” Gheorghe wrote on the internal messaging service that afternoon. The fix was constructed to look like routine server maintenance, so that NSO might continue to attempt attacks, providing Facebook with more data.

The next day, WhatsApp engineers said, NSO began to send what looked like decoy data packets, which they speculated were a way to determine whether NSO’s activities were being watched. “In one of the malicious packets, they actually sent a YouTube link,” Gheorghe told me. “We were all laughing like crazy when we saw what it was.” The link was to the music video for the Rick Astley song “Never Gonna Give You Up,” from 1987. Ambushing people with a link to the song is a popular trolling tactic known as Rickrolling. Otto Ebeling recalled, “Rickrolling is, I don’t know, something my colleague might do to me, not some sort of semi-state-sponsored people.” Cathcart told me, “There was a message in it. They were saying, We know what you did, we see you.” (Hulio and other NSO employees said they could not recall Rickrolling WhatsApp.)

In the months that followed, WhatsApp began notifying users who had been targeted. The list included numerous government officials, including at least one French ambassador and the Djiboutian Prime Minister. “There wasn’t, you know, overlap between this list and, like, legitimate law-enforcement outreach,” Cathcart said. “You could see, wow, there’s a lot of countries all around the world. This isn’t just one agency or organization in one country targeting people.” WhatsApp also began working with the Citizen Lab, which warned victims of the risk that they might be hacked again, and helped them secure their devices. John Scott-Railton said, “It really was interesting how many people were upset and

saddened, but in a deep way not surprised, almost relieved, as if they were getting a diagnosis for a mystery ailment they had suffered for many years.”

Five people in the initial group identified by WhatsApp were Catalans, including elected lawmakers and an activist. Campo, the Catalan security researcher, realized that the cases “were probably just the tip of the iceberg.” He added, “That’s when I found myself in the intersection of technology—a product that I contributed to building—and my home country.”

WhatsApp continued sharing information with the Department of Justice, and, that fall, the company sued NSO in federal court. NSO Group “breached our systems, damaged us,” Cathcart told me. “I mean, do you just do nothing about that? No. There have to be consequences.”

Hulio said, “I just remember that one day the lawsuit happened, and they shut down the Facebook account of our employees, which was a very bully move for them to do.” He added, referring to scandals about Facebook’s role in society, “I think it’s a big hypocrisy.” NSO has pushed for the suit to be dismissed, arguing that the company’s work on behalf of governments should grant it the same immunity from lawsuits that those governments have. So far, the U.S. courts have rejected this argument.

WhatsApp’s aggressive posture was unusual among big technology companies, which are often reluctant to call attention to instances in which their systems have been compromised. The lawsuit signalled a shift. The tech companies were now openly aligned against the spyware venders. Gheorghe described it as “the moment the whole thing just exploded.”

Microsoft, Google, Cisco, and others filed a legal brief in support of WhatsApp’s suit. Goodwin, the Microsoft executive, helped to assemble the coalition of companies. “We could not let NSO Group prevail with an argument that, simply because a government is using your products and services, you get sovereign immunity,” she told me. “The ripple effect of that would have been so dangerous.” Hulio argues that when governments use Pegasus they’re less likely to lean on platform holders for wider “back door” access to users’ data. He expressed exasperation with the lawsuit. “Instead of them, like, actually saying, ‘O.K., thank you,’ ” he told me, “they are going to sue us. Fine, so let’s meet in court.”

Microsoft, too, has a security team that engages in combat with hackers. Although Pegasus is not designed to target users through Microsoft platforms, at least four people in Catalonia running Microsoft Windows on their computers have been attacked by spyware made by Candiru, a startup founded by former NSO employees. (A spokesperson for Candiru said that it requires its products to be used for the “sole purpose of preventing crime and terror.”) In February, 2021, the Citizen Lab identified evidence of an active infection—a rarity for spyware of this calibre—on a laptop belonging to Joan Matamala, an activist closely connected to separatist politicians. Campo called Matamala and instructed him to wrap the laptop in aluminum foil, a makeshift way of blocking the malware from communicating with servers. The Citizen Lab was able to extract a copy of the spyware, which Microsoft dubbed DevilsTongue. Several months later, Microsoft released updates blocking DevilsTongue and preventing future attacks. By then, the list of activists and journalists targeted “made the hairs on the back of our neck stand on end,” Goodwin said. Matamala has been targeted more than sixteen times. “I still have the aluminum paper stored here, in case we ever have a suspicion of having another infection,” he told me.

Last November, after iPhone users were allegedly targeted by NSO, Apple filed its own lawsuit. NSO has filed a motion to dismiss. “Apple is a company that does not believe in theatrical lawsuits,” Ivan Krstić, the engineer, told me. “We have this entire time been waiting for a smoking gun that would let us go file a suit that is winnable.”

Apple created a threat-intelligence team nearly four years ago. Two Apple employees involved in the work told me that it was a response to the spread of spyware, exemplified by NSO Group. “NSO is a big pain point,” one of the employees told me. “Even before the stuff that hit the news, we had disrupted NSO a number of times.” In 2020, with the launch of its iOS 14 software, Apple had introduced a system called BlastDoor, which moved the processing of iMessages—including any potentially malicious code—into a chamber connected to the rest of the operating system by only a single, narrow pipeline of data. But Omer, the NSO V.P., told me that “newer features usually have some holes in their armor,” making them “more easy to target.” Krstić conceded that there was “a sort of an eye of a needle of an opening still left.”

In March, 2021, Apple’s security team received a tip that a hacker had successfully threaded that needle. Even cyber warfare has double agents. A person familiar with Apple’s threat-intelligence capabilities said that the company’s team sometimes receives tips from informants connected to spyware enterprises: “We’ve spent a long time and a lot of effort in trying to get to a place where we can actually learn something about what’s going on deeply behind the scenes at some of these companies.” (An Apple spokesperson said that Apple does not “run sources” within spyware companies.) The spyware venders, too, rely on intelligence gathering, such as securing pre-release versions of software, which they use to design their next attacks. “We follow the publications, we follow the beta versions of whatever apps we’re targeting,” Omer told me.

That month, researchers from the Citizen Lab contacted Apple: the phone of a Saudi women’s-rights activist, Loujain al-Hathloul, had been hacked through iMessage. Later, the Citizen Lab was able to send Apple a copy of an exploit, which the researcher Bill Marczak discovered after months of scrutinizing Hathloul’s phone, buried in an image file. The person familiar with Apple’s threat-intelligence capabilities said that receiving the file, through an encrypted digital channel, was “sort of like getting a thing handed to you in a biohazard bag, which says, ‘Do not open except in a Biosafety Level 4 lab.’ ”

Apple's investigation took a week and involved several dozen engineers based in the United States and Europe. The company concluded that NSO had injected malicious code into files in Adobe's PDF format. It then tricked a system in iMessage into accepting and processing the PDFs outside BlastDoor. "It's borderline science fiction," the person familiar with Apple's threat-intelligence capabilities said. "When you read the analysis, it's hard to believe." Google's security-research team, Project Zero, also studied a copy of the exploit, and later wrote in a blog post, "We assess this to be one of the most technically sophisticated exploits we've ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states." In the NSO offices, programmers in the Core Research Group printed a copy of the post and hung it on the wall.

Apple shipped updates for its platforms that rendered the exploit useless. Krstić told me that this was "a massive point of pride" for the team. But Omer told me, "We saw it coming. We just counted the days until it happened." He and others at the company said the next exploit is an inevitability. "There might be some gaps. It could take two weeks to come up with a mitigation on our side, some work-around."

During interviews in NSO's offices last month, employees exchanged nervous glances with hovering public-relations staffers as they answered questions about morale in the midst of the scandals, lawsuits, and blacklisting. "To be honest, not every time the mood is actually good," Omer said. Others claimed loyalty to the company and belief in the power of its tools to catch criminals. "The company has a very strong narrative that it tries to sell internally to the employees," the former employee told me. "You're either with them or against them."

Israel has become the world's most significant source of private surveillance technology in part because of the quality of talent and expertise produced by its military. "Because of the compulsory service, we can recruit the best of the best," the former senior intelligence official told me. "The American dream is going from M.I.T. to Google. The Israeli dream is to go to 8200," the Israeli military-intelligence unit from which spyware vendors often recruit. (Hulio, who describes himself as a mediocre student whose upbringing was "nothing fancy," often emphasizes that he did not serve in Unit 8200.) NSO has historically been regarded as an appealing job prospect for young veterans. But the former NSO employee, who quit after becoming concerned that Pegasus had facilitated Jamal Khashoggi's murder, told me that others had become disillusioned, too. "Many of my colleagues decided to leave the company at that stage," the former employee said. "This was one of the major events that I think caused many of the employees to, like, wake up and understand what's going on." In the past few years, the departures have been "like a snowball." Hulio, in response to questions about the company's problems, said, "What worries me is the vibes of the employees."

In 2019, NSO was saddled with hundreds of millions of dollars in debt as part of a leveraged-buyout deal in which a London-based private-equity firm, Novalpina, acquired a seventy-per-cent stake. Recently, Moody's, the financial-services firm, downgraded NSO's credit rating to "poor," and Bloomberg described it as a distressed asset, shunned by Wall Street traders. Two top NSO executives have left, and relations between the company and its backers have deteriorated. Infighting among Novalpina's partners led to the transfer of control of its assets, including NSO, to a consulting firm, Berkeley Research Group, which pledged to increase oversight. But a BRG executive recently claimed that cooperation with Hulio had become "virtually non-existent." Agence France-Presse has reported that tensions emerged because

NSO's creditors have pressed for continued sales to countries with dubious human-rights records, while BRG has sought to pause them. "We indeed have some disputes with them," Hulio said, of BRG. "It's about how to run the business."

NSO's troubles have complicated its close alliance with the Israeli state. The former senior intelligence official recalled that, in the past, when his unit turned down European countries seeking intelligence collaboration, "Mossad said, Here's the next best thing, NSO Group." Several people familiar with those deals said that Israeli authorities provided little ethical guidance or restraint. The former official added, "Israeli export control was not dealing with ethics. It was dealing with two things. One, Israeli national interest. Two, reputation." The former NSO employee said that the state "was well aware of the misuse, and even using it as part of its own diplomatic relationships." (Israel's Ministry of Defense said in a statement that "each licensing assessment is made in light of various considerations including the security clearance of the product and assessment of the country toward which the product will be marketed. Human rights, policy, and security issues are all taken into consideration.") After the blacklisting of NSO, Hulio sought to enlist Israeli officials, including Prime Minister Naftali Bennett and Defense Minister Benny Gantz. "I sent a letter," he told me. "I said that as a regulated company, you know, everything that we have ever asked was with the permission, and with the authority, of the government of Israel." But a senior Biden Administration official said that the Israelis raised only "pretty mild complaints" about the blacklisting. "They didn't like it, but we didn't have a standoff."

In Israel's legislature, Arab politicians are leading a modest movement to examine the state's relationship with NSO. The Arab party leader Sami Abou Shahadeh told me, "We tried to discuss this in the Knesset twice . . . to tell the Israeli politicians, You are selling death to very weak societies that are in conflict, and you've been doing this for too long." He added, "It never worked, because, first and morally, they don't see any problem with that." Last fall, an investigation by the watchdog group Front Line Defenders identified Pegasus infections on the phones of six Palestinian activists—including one whose Jerusalem residency status had been revoked. Abou Shahadeh argued that the history of Israel's spyware technology is tied to the surveillance of Palestinian communities in the West Bank, East Jerusalem, and Gaza. "They have a huge laboratory," he told me. "When they were using all the same tools for a long time to spy on Palestinian citizens, nobody cared." Asked about the targeting of Palestinians, Hulio said, "If Israel is using our tools to fight crime and terror, I would be very proud of it."

"I know there have been misuses," Hulio said. "It's hard for me to live with that. And I obviously feel sorry for that. Really, I'm not just saying that. I never said it, but I'm saying it now." Hulio said that the company has turned down ninety customers and hundreds of millions of dollars of business out of concern about the potential for abuse. But such claims are difficult to verify. "NSO wanted Western Europe mainly so they can tell guys like you, Here's a European example," the former Israeli intelligence official, who now works in the spyware sector, said. "But most of their business is subsidized by the Saudi Arabias of the world." The former employee, who had knowledge of NSO's sales efforts, said, "For a European country, they would charge ten million dollars. And for a country in the Middle East they could charge, like, two hundred and fifty million for the same product." This seemed to create perverse incentives: "When they understood that they had misuse in those countries that they sold to for enormous amounts of money, then the decision to shut down the service for that specific country became much, much harder."

Asked about the extreme abuses ascribed to his technology, Hudio invoked an argument that is at the heart of his company's defense against WhatsApp and Apple. "We have no access to the data on the system," he told me. "We don't take part in the operation, we don't see what the customers are doing. We have no way of monitoring it." When a client buys Pegasus, company officials said, an NSO team travels to install two racks, one devoted to storage and another for operating the software. The system then runs with only limited connection to NSO in Israel.

But NSO engineers concede that there is some real-time monitoring of systems to prevent unauthorized tampering with or theft of their technology. And the former employee said, of Hudio's assurances that NSO is technically prevented from overseeing the system, "That's a lie." The former employee recalled support and maintenance efforts that involved remote access by NSO, with the customer's permission and live oversight. "There is remote access," the former employee added. "They can see everything that goes on. They have access to the database, they have access to all of the data." The senior European law-enforcement official told me, "They can have remote access to the system when we authorize them to access the system."

NSO executives argue that, in an unregulated field, they are attempting to construct guardrails. They have touted their appointment of a compliance committee, and told me that they now maintain a list of countries ranked by risk of misuse, based on human-rights indicators from Freedom House and other groups. (They declined to share the list.) NSO also says that customers' Pegasus systems maintain a file that records which numbers were targeted; customers are contractually obligated to surrender the file if NSO starts an investigation. "We have never had a customer say no," Hudio told me. The company says that it can terminate systems remotely, and has done so seven times in the past few years.

The competition, Hudio argued, is far more frightening. "Companies found themselves in Singapore, in Cyprus, in other places that don't have real regulation," he told me. "And they can sell to whoever they want." The spyware industry is also full of rogue hackers willing to crack devices for anyone who will pay. "They will take your computers, they will take your phone, your Gmail," Hudio said. "It's obviously illegal. But it's very common now. It's not that expensive." Some of the technology that NSO competes with, he says, comes from state actors, including China and Russia. "I can tell you that today in China, today in Africa, you see the Chinese government giving capabilities almost similar to NSO." According to a report from the Carnegie Endowment for International Peace, China supplies surveillance tools to sixty-three countries, often through private firms enmeshed with the Chinese state. "NSO will not exist tomorrow, let's say," Hudio told me. "There's not going to be a vacuum. What do you think will happen?"

NSO is also competing with Israeli firms. Large-scale hacking campaigns, like the one in Catalonia, often use tools from a number of companies, several founded by NSO alumni. Candiru was started in 2014, by the former NSO employees Eran Shorer and Yaakov Weizman. It was allegedly linked to recent attacks on Web sites in the U.K. and the Middle East (Candiru denies the connection), and its software has been identified on the devices of Turkish and Palestinian citizens. Candiru has no Web site. The firm shares its name with a parasitic fish, native to the Amazon River basin, that drains the blood of larger fish.

QuaDream was founded two years later, by a group including two other former NSO employees, Guy Geva and Nimrod Reznik. Like NSO, it focusses on smartphones. Earlier this year, Reuters reported that QuaDream had exploited the same vulnerability that NSO used to gain access to Apple's iMessage.

QuaDream, whose offices are behind an unmarked door in the Tel Aviv suburb of Ramat Gan, appears to share with many of its competitors a reliance on regulation havens: its flagship malware, Reign, is reportedly owned by a Cyprus-based entity, InReach. According to *Haaretz*, the firm is among those now employed by Saudi Arabia. (QuaDream could not be reached for comment.)

Other Israeli firms pitch themselves as less reputationally fraught. Paragon, which was founded in 2018 by former Israeli intelligence officials and includes former Prime Minister Ehud Barak on its board, markets its technology to offices within the U.S. government. Paragon's core technology focusses not on seizing complete control of phones but on hacking encrypted messaging systems like Telegram and Signal. An executive told me that it has committed to sell only to a narrow list of countries with relatively uncontroversial human-rights records: "Our strategy is to have values, which is interesting to the American market."

**I**n Catalonia, Gonzalo Boye, an attorney representing nineteen people targeted by Pegasus, is preparing criminal complaints to courts in Spain and other European countries, accusing NSO, as well as Hulo and his co-founders, of breaking national and E.U. laws. Boye has represented Catalan politicians in exile, including the former President Carles Puigdemont. Between March and October of 2020, analysis by the Citizen Lab found, Boye was targeted eighteen times with text messages masquerading as updates from Twitter and news sites. At least one attempt resulted in a successful Pegasus infection. Boye says that he now spends as much time as possible outside Spain. In a recent interview, he wondered, "How can I defend someone, if the other side knows exactly everything I've said to my client?" Hulo declined to identify specific customers but suggested that Spain's use of the technology was legitimate. "Spain definitely has a rule of law," he told me. "And if everything was legal, with the approval of the Supreme Court, or with the approval of all the lawful mechanisms, then it can't be misused." Pere Aragonès, the current President of Catalonia, told me, "We are not criminals." He is one of three people who have served in that role whose phones have been infected with Pegasus. "What we want from the Spanish authorities is transparency."

Last month, the European Parliament formed a committee to look into the use of Pegasus in Europe. Last week, Reuters reported that senior officials at the European Commission had been targeted by NSO spyware. The investigative committee, whose members include Puigdemont, will convene for its first

session on April 19th. Puigdemont called NSO's activities "a threat not only for the credibility of Spanish democracy, but for the credibility of European democracy itself."

NSO Group also faces legal consequences in the U.K.: three activists recently notified the company, as well as the governments of Saudi Arabia and the U.A.E., that they plan to sue over alleged abuses of Pegasus. (The company responded that there was "no basis" for their claims.)

NSO continues to defend itself in the WhatsApp suit. This month, it filed an appeal to the U.S. Supreme Court. "If we need to go and fight, we will," Shmuel Sunray, NSO's general counsel, told me. Lawyers for WhatsApp said that, in their fight with NSO, they have encountered underhanded tactics, including an apparent campaign of private espionage.

On December 20, 2019, Joe Mornin, an associate at Cooley L.L.P., a Palo Alto law firm that was representing WhatsApp in its suit against NSO, received an e-mail from a woman who identified herself as Linnea Nilsson, a producer at a Stockholm-based company developing a documentary series on cybersecurity. Nilsson was cagey about her identity but so eager to meet Mornin that she bought him a first-class plane ticket from San Francisco to New York. The ticket was paid for in cash, through World Express Travel, an agency that specialized in trips to Israel. Mornin never used the ticket. A Web site for the documentary company, populated with photos from elsewhere on the Internet, soon disappeared. So did a LinkedIn profile for Nilsson.

Several months later, a woman claiming to be Anastasia Chistyakova, a Moscow-based trustee for a wealthy individual, contacted Travis LeBlanc, a Cooley partner working on the WhatsApp case, seeking legal advice. The woman sent voice-mail, e-mail, Facebook, and LinkedIn messages. Mornin identified her voice as belonging to Nilsson, and the law firm later concluded that her e-mail had come from the same block of I.P. addresses as those sent by Nilsson. The lawyers reported the incidents to the Department of Justice.

The tactics were similar to those used by the private intelligence company Black Cube, which is run largely by former officers of Mossad and other Israeli intelligence agencies, and is known for using operatives with false identities. The firm worked on behalf of the producer Harvey Weinstein to track women who had accused him of sexual abuse, and last month three of its officials received suspended prison sentences for hacking and intimidating Romania's chief anti-corruption prosecutor.

Black Cube has been linked to at least one other case involving NSO Group. In February, 2019, the A.P. reported that Black Cube agents had targeted three attorneys involved in another suit against NSO Group, as well as a London-based journalist covering the case. The lawyers—Mazen Masri, Alaa Mahajna, and Christiana Markou—who represented hacked journalists and activists, had sued NSO and an affiliated entity in Israel and Cyprus. In late 2018, all three received messages from people who claimed to be associated with a rich firm or individual, repeatedly suggesting meetings in London. NSO Group has denied hiring Black Cube to target opponents. However, Hudio acknowledged the connection to me, saying, "For the lawsuit in Cyprus, there was one involvement of Black Cube," because the lawsuit "came from nowhere, and I want to understand." He said that he had not hired Black Cube for other lawsuits. Black Cube said that it would not comment on the cases, though a source familiar with the company denied that it had targeted Cooley lawyers.

“People can survive and can adapt to almost any situation,” Hudio once told me. NSO Group must now adapt to a situation in which its flagship product has become a symbol of oppression. “I don’t know if we’ll win, but we will fight,” he said. One solution was to expand the product line. The company demonstrated for me an artificial-intelligence tool, called Maestro, that scrutinizes surveillance data, builds models of individuals’ relationships and schedules, and alerts law enforcement to variations of routine that might be harbingers of crime. “I’m sure this will be the next big thing coming out of NSO,” Leoz Michaelson, one of its designers, told me. “Turning every life pattern into a mathematical vector.”

The product is already used by a handful of countries, and Hudio said that it had contributed to an arrest, after a suspect in a terrorism investigation subtly altered his routine. The company seemed to have given little consideration to the idea that this tool, too, might spur controversy. When I asked what would happen if law enforcement arrested someone based on, say, an innocent trip to the store in the middle of the night, Michaelson said, “There could be false positives.” But, he added, “this guy that is going to buy milk in the middle of the night is in the system for a reason.”

Yet the risk to bystanders is not an abstraction. Last week, Elies Campo decided to check the phones of his parents, scientists who are not involved in political activities, for spyware. He found that both had been infected with Pegasus when he visited them during the Christmas holiday in 2019. Campo told me, “The idea that anyone could be at risk from Pegasus wasn’t just a concept anymore—it was my parents sitting across the table from me.” On his mother’s phone, which had been hacked eight times, the researchers found a new kind of zero-click exploit, which attacked iMessage and iOS’s Web-browsing engine. There is no evidence that iPhones are still vulnerable to the exploit, which the Citizen Lab has given the working name *Homage*. When the evidence was found, Scott-Railton told Campo, “You’re not going to believe this, but your mother is patient zero for a previously undiscovered exploit.”

During a recent visit to NSO’s offices, windows and whiteboards across the space were dense with flowcharts and graphics, in Hebrew and English text, chronicling ideas for products and exploits. On one whiteboard, scrawled in large red Hebrew characters and firmly underlined, was a single word: “War!” ♦

*Georgia Gee conducted additional research for this piece.*

An earlier version of this story misstated the time of a Pegasus infection on a device connected to the network at 10 Downing Street.

*Published in the print edition of the April 25 & May 2, 2022 issue, with the headline “The Surveillance States.”*

---

## NEW YORKER FAVORITES

---

- The book that inspired Disney’s “Bambi” is even darker than the cartoon—and has an unsettling message about humanity.
- A Cambridge classicist takes on her sexist detractors.
- Does wisdom really come from experience?
- The trans swimmer who won too much.

- The mind behind “Where the Wild Things Are.”
- From 1938: Alfred Hitchcock’s many plans.

Sign up for our daily newsletter to receive the best stories from *The New Yorker*.



Ronan Farrow, a contributing writer to *The New Yorker*, is the author of “Catch and Kill” and “War on Peace.” His reporting for *The New Yorker* won the 2018 Pulitzer Prize for public service.

More: [Surveillance](#) [Technology](#) [Tech Companies](#) [Cybersecurity](#) [Israel](#) [Spain](#) [Intelligence](#) [Hacking](#) [WhatsApp](#) [Facebook](#) [Apple](#)  
[Software](#)

## THIS WEEK’S ISSUE

Never miss a big *New Yorker* story again. Sign up for This Week’s Issue and get an e-mail every week with the stories you have to read.

E-mail address

Your e-mail address

Sign up

By signing up, you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#).

[Cookies Settings](#)

## יפוי כח

אנו, מורשי החתימה של כלכליסט-ידיעות אחרונות בע"מ, מיפים את מוחם של עוה"ד ט. ליבליך ו/או מ. כץ ו/או אח' להיות באי - הכוח בעניין ת"א קבוצת או אס או טכנולוגיות בע"מ נ' כלכליסט ואח' ובכל דבר ועניין הקשור לחליף זה:

מבלי לפגוע בכלליות המינוי הנ"ל יהיו באי הכח רשאים לעשות ולפעול בשם ובמקום כלכליסט בכל הפעולות הבאות, כולן או מקצתן הכל בקשר לעניינים הנ"ל ולכל הנובע מהם כדלקמן:

1. לחתום על ולהגיש בשם כלכליסט כל תביעה או תביעה שכנגד, ו/או כל בקשה, הגנה, התנגדות, בקשה למן רשות ערעור, ערעור, דיון נוסף, חידעה, טענה, השגה, ערר, תובענה או חליף אחר הנוגע או הנובע מהחליף הנ"ל ללא יוצא מן הכלל. כמו כן להודות ו/או לכפור בשם כלכליסט בכתב אישום במשפטים פליליים בנוכחותנו או בהעדרנו.
2. להזמין עדים, למנות מומחים, ולעשות כל הפעולות לפי תקנות סדרי הדין הקיימים כיום ושיהיו קיימים בעתיד, או לבצע כל הפעולות בתוקף כל חוק או פרצדורה אחרת שחלה או שתחול על התביעה או על המשפט הנ"ל.
3. לחתום ולשלוח תראות מכל סוג, לדרוש הכרזת פשיטת רגל, ו/או פירוק גוף משפטי מכל סוג שהוא ולעשות את כל הפעולות הקשורות והנובעות מהענין הנ"ל.
4. להופיע בשם כלכליסט ולייצגו בקשר לכל אחת מהפעולות הנ"ל בפני כל בתי המשפט, בתי דין למיניהם או רשויות ומוסדות אחרים הן ממשלתיים והן אחרים, עד לדרגתם האחרונה.
5. למסור כל ענין הנוגע או הנובע מהעניין האמור לעיל לבוררות ולחתום על שטר בוררים כפי שבאי הכח ימצאו לנכון ולמועיל.
6. להתפשר בכל ענין הנוגע או הנובע מהעניינים האמורים לעיל לפי שקול דעתם של בא הכח ולחתום על פשרה כזו בבית המשפט או מחוצה לו.
7. לגבות את סכום התביעה או כל סכום אחר בכל ענין מהעניינים הנ"ל לרבות תוצאות בית משפט ושכר טרחת עו"ד. לקבל בשם ובמקום כלכליסט כל מסמך והפך ולתת קבלות ושחרורים כפי שבאי הכח ימצאו לנכון ולמתאים.
8. להוציא לפועל כל פס"ד או החלטה או צו, לדרוש צווי מכירה, עיקולים או פקודות מאסר ולעשות כל הפעולות המותרות על פי חוק ההוצאה לפועל ו/או התקנות על פיו.
9. לנקוט בכל הפעולות ולחתום על כל מסמך או כתב בלי יוצא מן הכלל כפי שבאי הכח ימצאו לנכון בכל ענין הנובע מהענין הנ"ל.
10. להופיע בשם כלכליסט ולייצגו בענין הנ"ל בפני כל רשות ממשלתית ו/או ציבורית לרבות האפוטרופוס הכללי, הרשם לענייני ירושה, רשם המקרקעין, לשכת רישום המקרקעין, שלטונות המס, עיריות ומועצות מקומיות, לחתום בשמי ובמקומי על כל בקשה, הצהרה הערות אזהרה ומסמכים אחרים למיניהם ולבצע בשמי כל עסקה המוכרת על פי דין וליתן הצהרות, קבלות ואשורים ולקבל בשמו ובמקומו כל מסמך שהוא רשאי לקבלו על פי דין.
11. להופיע בשם כלכליסט ולייצגו בענין הנ"ל בפני רשם החברות, רשם השותפויות ורשם האגודות השיתופיות, לחתום במקומו על כל בקשה או מסמך אחר בקשר לרשום גוף משפטי, לטפל ברישומו או מחיקתו של כל גוף משפטי ולטפל בכל דבר הנוגע לו ולבצע כל פעולה בקשר לאותו גוף משפטי.
12. להופיע בשם כלכליסט ולייצגו בכל תביעה ייצוגית על פי תקנות סדר הדין ועל פי כל חוק.
13. לחתום בשמו על יפוי כח בלתי חוזרים.
14. למנות כל עורך דין לשמש במקומו בכל משא ומתן משפטי לפי יפוי כח זה.
15. להעביר את הסמכויות שביפוי כח זה, כולן או מקצתן, לעו"ד אחר עם זכות העברה לאחרים. למנות ולפטר עו"ד ולמנות אחרים במקומם.
16. לנהל את ענייניו הנ"ל של כלכליסט לפי ראות עינו ובאופן שימצא לנכון ולמועיל בקשר עם ענייני הנ"ל.
17. הנני מאשר/ת את מעשי באי הכח או מעשי ממלאי מקומם בתוקף יפוי כח זה מראש.

הכתוב דלעיל ביחיד יכול את הרבים להפיך.

ולראיה באתי על החתום, היום 3 בחודש 1/11 שנת 2022.

חתימה  
איל פאר מנכ"ל כלכליסט

חתימה  
עורך הדין

הנני מאשר את חתימת מרשתי הנ"ל

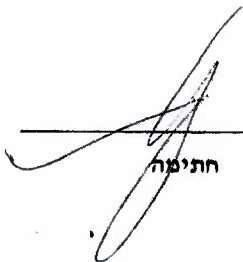
## יפוי כח

אני החתומה מטה גלית חמי מס' ת.ז. 23798101, מיפה את כוחם של עוה"ד ט. ליבליך ו/או מ. כץ להיות באי - כוחי בעניין ת"א קבוצת אן אס אוו טכנולוגיות בע"מ נ' כלכליסט ואח' ובכל דבר ועניין הקשור להליך זה:

מבלי לפגוע בכלליות המינוי הנ"ל יהיו באות כחי רשאויות לעשות ולפעול בשמי ובמקומי בכל הפעולות הבאות, כולן או מקצתן הכל בקשר לעניינים הנ"ל ולכל הנובע מהם כדלקמן:

1. לחתום על ולהגיש בשמי כל תביעה או תביעה שכנגד, ו/או כל בקשה, הגנה, התנגדות, בקשה למן רשות ערעור, ערעור, דיון נוסף, הודעה, טענה, השגה, ערר, תובענה או הליך אחר הנוגע או הנובע מההליך הנ"ל ללא יוצא מן הכלל. כמו כן להודות ו/או לכפור בשמי בכתב אישום במשפטים פליליים בנוכחותי או בהעדרנו.
2. להזמין עדים, למנות מומחים, ולעשות כל הפעולות לפי תקנות סדרי הדין הקיימים כיום ושיהיו קיימים בעתיד, או לבצע כל הפעולות בתוקף כל חוק או פרוצדורה אחרת שחלה או שתחול על התביעה או על המשפט הנ"ל.
3. לחתום ולשלוח התראות מכל סוג, לדרוש הכרזת פשיטת רגל, ו/או פירוק גוף משפטי מכל סוג שהוא ולעשות את כל הפעולות הקשורות והנובעות מהענין הנ"ל.
4. להופיע בשמי ולייצגני בקשר לכל אחת מהפעולות הנ"ל בפני כל בתי המשפט, בתי דין למיניהם או רשויות ומוסדות אחרים הן מממשלתיים והן אחרים, עד לדרגתם האחרונה.
5. למסור כל ענין הנוגע או הנובע מהענין האמור לעיל לבוררות ולחתום על שטר בוררים כפי שבא כחי ימצא לנכון ולמועיל.
6. להתפשר בכל ענין הנוגע או הנובע מהעניינים האמורים לעיל לפי שקול דעתו של בא כחי ולחתום על פשרה כזו בבית המשפט או מחוצה לו.
7. לגבות את סכום התביעה או כל סכום אחר בכל ענין מהעניינים הנ"ל לרבות הוצאות בית משפט ושכר טרחת עו"ד. לקבל בשמי ובמקומי כל מסמך וחפץ ולחתם קבלות ושחרורים כפי שבא כחי ימצא לנכון ולמתאים.
8. להוציא לפועל כל פס"ד או החלטה או צו, לדרוש צווי מכירה, עיקולים או פקודות מאסר ולעשות כל הפעולות המותרות על פי חוק ההוצאה לפועל ו/או התקנות על פיו.
9. לנקוט בכל הפעולות ולחתום על כל מסמך או כתב בלי יוצא מן הכלל כפי שבאות כחי ימצאו לנכון בכל ענין הנובע מהענין הנ"ל.
10. להופיע בשמי ולייצגני בענין הנ"ל בפני כל רשות ממשלתית ו/או ציבורית לרבות האפוטרופוס הכללי, הרשם לענייני ירושה, רשם המקרקעין, לשכת רישום המקרקעין, שלטונות המס, עיריות ומועצות מקומיות, לחתום בשמי ובמקומי על כל בקשה, הצהרה הערות אזהרה ומסמכים אחרים למיניהם ולבצע בשמי כל עסקה המוכרת על פי דין וליתן הצהרות, קבלות ואשורים ולקבל בשמי ובמקומי כל מסמך שאני רשאי לקבלו על פי דין.
11. להופיע בשמי ולייצגני בענין הנ"ל בפני רשם החברות, רשם השותפויות ורשם האגודות השיתופיות, לחתום במקומי על כל בקשה או מסמך אחר בקשר לרשום גוף משפטי, לטפל ברישומי או מחיקתו של כל גוף משפטי ולטפל בכל דבר הנוגע לו ולבצע כל פעולה בקשר לאותו גוף משפטי.
12. להופיע בשמי ולייצגני בכל תביעה ייצוגית על פי תקנות סדר הדין ועל פי כל חוק.
13. לחתום בשמי על יפוי כח בלתי חוזרים.
14. למנות כל עורך דין לשמש במקומן בכל משא ומתן משפטי לפי יפוי כח זה.
15. להעביר את הסמכויות שביפוי כח זה, כולן או מקצתן, לעו"ד אחר עם זכות העברה לאחרים. למנות ולפטר עו"ד ולמנות אחרים במקומם.
16. לנהל את עניני הנ"ל לפי ראות עינן ובאופן שימצא לנכון ולמועיל בקשר עם עניני הנ"ל.
17. הנני מאשר את מעשי באות כחי או מעשי ממלאי מקומן בתוקף יפוי כח זה מראש. הכתוב דלעיל ביחיד יכלול את הרבים ולהיפך.

ולראיה באתי על החתום, היום 2 בחודש אלול שנת 2022.

  
חתימה

  
חתימה  
עורך הדין

הנני מאשר את חתימת מרשי הנ"ל

## יפוי כח

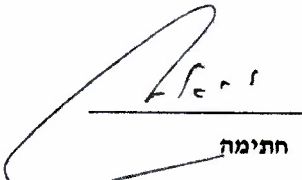
אני החתום מטה יואל אסתרן מס' ת.ז. 51286425, מיפה את כוחם של עוה"ד ט. ליבליך ו/או מ. כץ להיות באי - כוחי בעניין ת"א קבוצת אן אס אוו טכנולוגיות בע"מ נ' כלכליסט ואח' ובכל דבר ועניין הקשור להליך זה:


מבלי לפגוע בכלליות המינוי הנ"ל יהיו באות כחי רשאיות לעשות ולפעול בשמי ובמקומי בכל הפעולות הבאות, כולן או מקצתן הכל בקשר לעניינים הנ"ל ולכל הנובע מהם כדלקמן:

1. לחתום על ולהגיש בשמי כל תביעה או תביעה שכנגד, ו/או כל בקשה, הגנה, התנגדות, בקשה למן רשות ערעור, ערעור, דיון נוסף, הודעה, טענה, השגה, ערר, תובענה או הליך אחר הנוגע או הנובע מההליך הנ"ל ללא יוצא מן הכלל. כמו כן להודות ו/או לכפור בשמי בכתב אישום במשפטים פליליים בנוכחותי או בהעדרנו.
2. להזמין עדים, למנות מומחים, ולעשות כל הפעולות לפי תקנות סדרי הדין הקיימים כיום ושיהיו קיימים בעתיד, או לבצע כל הפעולות בתוקף כל חוק או פרוצדורה אחרת שחלה או שתחול על התביעה או על המשפט הנ"ל.
3. לחתום ולשלוח התראות מכל סוג, לדרוש הכרזת פשיטת רגל, ו/או פירוק גוף משפטי מכל סוג שהוא ולעשות את כל הפעולות הקשורות והנובעות מהענין הנ"ל.
4. להופיע בשמי ולייצגני בקשר לכל אחת מהפעולות הנ"ל בפני כל בתי המשפט, בתי דין למיניהם או רשויות ומוסדות אחרים הן ממשלתיים והן אחרים, עד לדרגתם האחרונה.
5. למסור כל ענין הנוגע או הנובע מהענין האמור לעיל לבוררות ולחתום על שטר בוררים כפי שבא כחי ימצא לנכון ולמועיל.
6. להתפטר בכל ענין הנוגע או הנובע מהעניינים האמורים לעיל לפי שקול דעתו של בא כחי ולחתום על פשרה כזו בבית המשפט או מחוצה לו.
7. לגבות את סכום התביעה או כל סכום אחר בכל ענין מהעניינים הנ"ל לרבות הוצאות בית משפט ושכר טרחת עו"ד. לקבל בשמי ובמקומי כל מסמך וחפץ ולתת קבלות ושחרורים כפי שבא כחי ימצא לנכון ולמתאים.
8. להוציא לפועל כל פס"ד או החלטה או צו, לדרוש צווי מכירה, עיקולים או פקודות מאסר ולעשות כל הפעולות המותרות על פי חוק ההוצאה לפועל ו/או התקנות על פיו.
9. לנקוט בכל הפעולות ולחתום על כל מסמך או כתב בלי יוצא מן הכלל כפי שבאות כחי ימצאו לנכון בכל ענין הנובע מהענין הנ"ל.
10. להופיע בשמי ולייצגני בענין הנ"ל בפני כל רשות ממשלתית ו/או ציבורית לרבות האפוטרופוס הכללי, הרשם לענייני ירושה, רשם המקרקעין, לשכת רישום המקרקעין, שלטונות המס, עיריות ומועצות מקומיות, לחתום בשמי ובמקומי על כל בקשה, הצהרה הערות אזהרה ומסמכים אחרים למיניהם ולבצע בשמי כל עסקה המוכרת על פי דין וליתן הצהרות, קבלות ואשורים ולקבל בשמי ובמקומי כל מסמך שאני רשאי לקבלו על פי דין.
11. להופיע בשמי ולייצגני בענין הנ"ל בפני רשם החברות, רשם השותפויות ורשם האגודות השיתופיות, לחתום במקומי על כל בקשה או מסמך אחר בקשר לרשום גוף משפטי, לטפל ברישומי או מחיקתו של כל גוף משפטי ולטפל בכל דבר הנוגע לו ולבצע כל פעולה בקשר לאותו גוף משפטי.
12. להופיע בשמי ולייצגני בכל תביעה ייצוגית על פי תקנות סדר הדין ועל פי כל חוק.
13. לחתום בשמי על יפוי כח בלתי חוזרים.
14. למנות כל עורך דין לשמש במקומן בכל משא ומתן משפטי לפי יפוי כח זה.
15. להעביר את הסמכויות שביפוי כח זה, כולן או מקצתן, לעו"ד אחר עם זכות העברה לאחרים. למנות ולפטר עו"ד ולמנות אחרים במקומם.
16. לנהל את עניני הנ"ל לפי ראות עינן ובאופן שימצא לנכון ולמועיל בקשר עם עניני הנ"ל.
17. הנני מאשר את מעשי באות כחי או מעשי ממלאי מקומן בתוקף יפוי כח זה מראש.

הכתוב דלעיל ביחיד יכול את הרבים להיפך.

ולראיה באתי על החתום, היום 2 בחודש אלול' שנת 2022.

  
חתימה

  
עו"ד הדין

הנני מאשר את חתימת מרשי הנ"ל