



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

20 יולי 2015
סימוכין: 083-4

לכבוד:

ח"כ סילבן שלום – שר הפנים

מר אמנון בן עמי – מנכ"ל רשות האוכלוסין וההגירה

מר גון קמני – ראש הרשות לניהול המאגר הביומטרי

א.נ.

הנדון: הממונה על היישומים הביומטריים - דו"ח פיקוח מסכם לתקופת המבחן 30.6.2013-30.6.2015
חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע,

התש"ע – 2009

סימוכין: 1. תכנית הפיקוח (o0103 מה- 26.6.13)

2. דו"ח פיקוח מס' 1 (or036 מה- 16.2.14)

3. דו"ח פיקוח מס' 2 (or065_5 מה- 28.1.2015)

4. דו"ח מסכם והמלצות לקראת תום "תקופת המבחן" -

הוועדה המייעצת המפקחת על התנהלות תקופת המבחן ובחינת תוצאותיה 28.5.2015

בהתאם לסמכות הפיקוח של הממונה על היישומים הביומטריים במשרד ראש הממשלה (להלן – "הממונה") על פי סעיף 30(ב)(3) לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009 (להלן – "החוק") ולתכנית הפיקוח שבסימוכין 1, מגיש בזאת הממונה דו"ח פיקוח מסכם (להלן – "הדו"ח") לתקופת המבחן.

טיוטת הדו"ח הועברה להתייחסות מקדימה של רשות האוכלוסין וההגירה ומעברי הגבול (להלן – "רשות א"), הרשות לניהול המאגר הביומטרי (להלן – "רשות ב"), הרשות למשפט וטכנולוגיה (להלן – "רשות ג") והחטיבה לסיכול איומי הסייבר בשב"כ (קרויה גם רא"מ) (להלן – "החטיבה"). התייחסותם מובאת בנספח ד' לדו"ח.

אנא שימו לב שנספח ב' בדו"ח, מסווג סודי. יתר הדו"ח מסווג בלמ"ס.

1. רקע:

1.1. סעיף 30(ב)(3) לחוק קובע כי על הממונה "לפקח על יישום הוראות חוק זה והתקנות, הכללים, הנחיות הרשות ונוהלי הרשות אשר נקבעו מכוחו, וכן על פעולות ראש הרשות לפי חוק זה". בהתאם לסעיף זה נערך תהליך פיקוח (ראו פירוט להלן) על פרויקט התייעוד החכם, ממועד תחילתו של הפרויקט.

1.2. דו"ח הפיקוח המסכם של הממונה, הוא הדו"ח השלישי המוגש על ידי הממונה, מציג את ממצאי הפיקוח העיקריים, במהלך תקופת המבחן ואת הפערים שנשארו פתוחים במועד כתיבת הדו"ח.

1.3. פרויקט החלפת תעודות הזהות והדרכונים של תושבי מדינת ישראל בתעודות זהות ודרכונים חכמים משולבי ביומטריה, תוכנן ומבוצע על ידי משרד הפנים, בהתאם למתווה הקבוע בחוק. הפרויקט יצא לדרך ב-30 ביוני 2013. כ-40% מהתושבים העדיפו לבחור בתייעוד חכם בתקופת המבחן, מבין אלו שהחליפו או הנפיקו תעודות זהות ודרכונים. נכון ליוני 2015 נכללו במאגר הביומטרי כ-700,000 איש.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

- 1.4. ניתן לומר ששיטת החלפת התייעוד מתקדמת בקצב מהיר והרשויות המבצעות את הפרויקט מממשות אותו בהצלחה.
- 1.5. הפרויקט כולל גם מאגר ביומטרי אשר הוקם ומופעל באחריות רשות ב' ומשימתו העיקרית **למנוע הרכשה כפולה**. סעיף 41 לחוק קבע כי תתקיים תקופת מבחן אשר תבחן את נחיצות קיומו של המאגר ומטרותיו, את המידע שיש לשמור בו ואת אופן השימוש בו (להלן – "תקופת המבחן").
- 1.6. תקופת המבחן מנוהלת בהתאם לצו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע (תקופת מבחן) תשע"א 2011 (להלן: "צו המבחן") ובהתאם לפרוטוקול המבחן.
- 1.7. בסוף מרץ 2015, הוגש דיווח ראש הממשלה ושר הפנים לוועדת השרים ליישומים ביומטריים ולוועדות הכנסת בהתאם לסעיף 41(4) לחוק. לדיווח זה צורפו דו"ח רשות א' ודו"ח רשות ב' אשר כללו את סקירתן לממצאי תקופת המבחן והמלצותיהן של הרשויות בהקשר לנחיצות המאגר והמידע שיש לשמור בו. בדו"חות אלה המליצו הרשויות להחיל את החוק על תושבי ישראל ולבחור בחלופת "המאגר המלא" אשר יכלול טביעות אצבע ותמונות פנים.
- 1.8. בפניית ראש הממשלה ושר הפנים למזכיר הממשלה וליו"ר הכנסת, להגשת הדיווח, נכתב כי המלצות הרשויות "ישקלו על ידי שר הפנים לעת הפעלת סמכותו על פי סעיף 41(5) לחוק, לצורך מתן הצו בהתאם לסעיף האמור". מתן צו לפי סעיף 41(5) לחוק משמעותו קבלת החלטה ביחס לממצאי תקופת המבחן ולמאגר הביומטרי.
- 1.9. **הוועדה המייעצת המפקחת על תקופת המבחן, שמונתה על ידי שר הפנים לפי סעיף 10ד לצו המבחן, ואשר בראשה עומד הממונה (להלן "הוועדה המייעצת")** הגישה לשר הפנים ביום 28.5.15 דו"ח מסכם והמלצות לקראת תום תקופת המבחן" (סימוכין 4).
- 1.10. דו"ח הוועדה המייעצת כולל התייחסות לסוגיות שנדונו על ידה לאורך תקופת המבחן וכן המלצות הנוגעות לפרויקט ובפרט לגבי המאגר הביומטרי, נחיצותו והמידע שיש לשמור בו. הוועדה המייעצת המליצה להימנע מהארכת תקופת המבחן, לקבוע כי יש נימוקים המבססים את נחיצות המאגר הביומטרי כאשר מאגר זה יכיל תמונות פנים בלבד, ללא טביעות אצבע, וכן המלצות נוספת לאורך חייו של הפרויקט. הוועדה המייעצת נעזרה ביחידת הממונה וביועציה לבדיקות המקצועיות שנדרשו לצורך ניהול דיוניה וגיבוש מסקנותיה.
- 1.11. דו"ח **הפיקוח המסכם של הממונה שיפורט להלן** מציג את התייחסותו הכוללת של הממונה מכוח סמכות הפיקוח הנתונה לו בחוק, בנפרד מפעילות הוועדה המייעצת ובנוסף עליה. הנושאים המרכזיים המופיעים בדו"ח זה קיבלו גם את התייחסותה של הוועדה המייעצת בדו"ח שהגישה.
- 1.12. במועד כתיבת דו"ח הפיקוח המסכם, פורסם גם דו"ח מבקר המדינה העוסק ב"תקופת המבחן". מבקר המדינה פנה אל הממונה במהלך תקופת המבחן וניהול הליך הפיקוח של הממונה, ועדכן כי בכוונתו לבצע הליך ביקורת מטעמו על תקופת המבחן. לצורך ביצוע הליך הביקורת של המבקר, העבירה יחידת הממונה, לבקשתו של מבקר המדינה, מסמכים רבים, המתארים את המעקב והפיקוח המבוצע על ידי הממונה והוועדה, בפרט ביחס לתקופת המבחן וסוגיות מרכזיות שנבדקו על ידם. סוגיות אלה מופיעות גם בדו"ח מבקר המדינה ולגביהן תינתן התייחסות עדכנית בדו"ח מסכם זה.
- 1.13. בימים אלה אישרה הכנסת את צו שר הפנים להארכת תקופת המבחן בתשעה חודשים נוספים, בהתאם לתהליך שנקבע בסעיף 41(5) לחוק.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

2. מטרות הדו"ח:

- 2.1. הצגת הנושאים העיקריים שנבדקו ע"י הממונה במהלך תקופת המבחן, דרך הטיפול בנושאים אלו, הפערים הפתוחים ומשמעותם בעת הזאת.
- 2.2. התייחסות לדו"חות המסכמים של שתי הרשויות.
- 2.3. התייחסות לדו"ח מבקר המדינה
- 2.4. המלצות הממונה על היישומים הביومترיים לסוף תקופת המבחן

3. מבנה המסמך:

- 3.1. עיקרי פעילויות הפיקוח שבוצעו, מוצגים בסעיף 4 להלן.
- 3.2. עיקרי הממצאים מוצגים בסעיף 5 להלן, המהווה את "תקציר המנהלים" של הדו"ח.
- 3.3. הממצאים המפורטים מוצגים בנספחים הבאים:
 - 3.3.1. נספח א' מציג את עיקרי ממצאי הפיקוח הכלליים ובתחום הפונקציונאלי של הביומטריה, והמעקב אחריהם.
 - 3.3.2. נספח ב' מציג את עיקרי ממצאי הפיקוח בתחום אבטחת המידע – נספח זה מסווג "סודי".
 - 3.3.3. נספח ג' מציג את עיקרי ממצאי הפיקוח בתחום הגנת הפרטיות וכבוד האדם, והמעקב אחריהם.
 - 3.3.4. נספח ד' מציג את תגובת הרשויות לדו"ח.
 - 3.3.5. נספח ה' מציג את הנתונים עליהם מבוססת המלצת הוועדה המייעצת בנוגע למאגר מבוסס על תמונות פנים בלבד.

4. תיאור עיקרי פעילויות הפיקוח שבוצעו במהלך תקופת המבחן:

- 4.1. תהליך הפיקוח בוצע בהתאם לתכנית הפיקוח (סימוכין 1), אשר גובשה על ידי הממונה.
- 4.2. תכנית הפיקוח תואמה עם החטיבה לסיכול איומי הסייבר בשב"כ (קרויה גם רא"מ) (להלן – "החטיבה"), הרשות למשפט וטכנולוגיה (להלן – "רמו"ט") מטה הסייבר הלאומי והתקשוב הממשלתי. לאחר מכן הועברה תכנית הפיקוח גם להתייחסות הרשויות, ותגובתן נשקלה לצורך גיבוש הסופי של התכנית.
- 4.3. התקיימו פגישות עבודה בין יחידת הממונה לרשויות המפוקחות בהן הוצגו ונדונו נושאים שבפיקוח.
- 4.4. נערכו סיורים, בלשכות רשות א', ביחידת "ארבל", במפעל "פתקית" וברשב"ג, וכן ברשות לניהול המאגר הביומטרי, בהם נבחנו תהליכי העבודה של גופים אלו בהתייחס לחוק, לתקנות, לצו ולפרוטוקול.
- 4.5. הפיקוח בוצע בשיתוף פעולה עם החטיבה ועם רמו"ט.
- 4.6. התקיימה עבודה מול המשטרה, משרד החוץ וגורמים נוספים לפי הצורך ובהתאם לנושאים שבאחריותם.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

5. עיקרי הממצאים

במהלך תקופת המבחן חיברה יחידת הממונה שני דו"חות פיקוח (סימוכין 2 ו-3), אשר הוגשו לשר הפנים, דו"ח פיקוח 2 הוגש גם לסגנית השר דאז ולראשי הרשויות. בשני דו"חות הפיקוח הוצגו פערים אשר הרשויות התבקשו לפעול לסגירתם. להלן פירוט הנושאים אותם מצאה יחידת הממונה לציין בדו"חות והפערים שנשארו בעת הגשת הדו"ח הנוכחי.

סעיף 5.5 מפרט את הנושאים אשר נותרו כפער במועד דו"ח זה.

5.1. נושאים כלליים ונושאי ביומטריה

5.1.1. תכנית עבודה מפורטת ולוחות זמנים

דו"ח הפיקוח הראשון ציין את הצורך בהצגת תכנית עבודה מפורטת, ככלי שנועד לסייע לרשויות להתכנס ללוחות זמנים באופן מסודר, וכדי לוודא את התנהלות התקינה של תקופת המבחן וסיום כל הפעילויות הנדרשות במהלכה.

תכנית העבודה המפורטת הוגשה בעיכוב של מספר חודשים. בדו"ח הפיקוח השני צוין כי הפער בנושא זה קיבל מענה, כאשר התכנית הוגשה על ידי הרשויות באופן המאפשר מעקב ועמידה בלוחות זמנים. תכנית העבודה הוצגה בפני הוועדה המייעצת ובפני צוות הפיקוח של יחידת הממונה.

מתחילה, תכנית העבודה המפורטת הייתה משותפת לשתי הרשויות, אולם החל מחודש אוגוסט 2014 התכנית פוצלה והוגשו שתי תכניות עבודה, לכל רשות בנפרד. דו"ח הפיקוח השני ביקש לוודא שיש בידי ועדת ההיגוי של הפרויקט במשרד הפנים תכנית עבודה כוללת של הפרויקט בשתי הרשויות.

בנושא זה ציינה רשות א' כי תכניות שתי הרשויות הוצגו בפני וועדת ההיגוי במשרד הפנים. לקראת הגשת הדו"חות המסכמים של הרשויות, נמסר לנו שמר אבי חליבה – סמנכ"ל במשרד הפנים מונה על ידי שר הפנים להיות הגורם המתכלל בפרויקט.

נושא זה הוזכר בדו"ח המבקר ובמועד כתיבת דו"ח פיקוח 2, כבר לא נמצא בו פער.

5.1.2. תקפות ממצאי תקופת המבחן בהתבסס על מערכת הביניים "להב"

תקופת המבחן החלה על גבי מערכת זמנית "להב". מתחילה תוכנן לבצע את תקופת המבחן על גבי מערכת בתצורה סופית "מגן". עיכוב במכרז למערכת "מגן" גרם לכך שכל תקופת המבחן התנהלה על גבי מערכת "להב". סוגיה זו טופלה על ידי יחידת הממונה מכמה היבטים:

1. האם מערכת "להב" מסוגלת לשאת על גבה את כמות ההרכשות עד עלות מערכת "מגן" לעבודה ביצור, ולייצר נתונים תוצאתיים מספקים לבדיקת החלופות בתקופת המבחן.
2. האם תוצאות תקופת המבחן עלולות להיות שונות לאור זאת שבתקופת המבחן תיבדק מערכת "להב" לעומת בדיקה באמצעות מערכת "מגן".

בסופה של הבחינה, שוכנעה יחידת הממונה שמערכת "להב" מסוגלת לשאת את כמות ההרכשות הצפויה והפקת נתונים, וכן שהחלטות שיתקבלו על גבי מערכת "להב" יהיו תקפות עבור תקופת המבחן וזאת לאחר שהתקבלו מסמכים והסברים מהיועץ הביומטרי של רשות ב' וממומחי מחצ"ב רפא"ל, ומבדיקת מומחי יחידת הממונה, שבדקו ואישרו קביעה זאת.

נושא זה נבדק גם על ידי הוועדה המייעצת לאורך מספר דיונים, בהם הופיעו בפניה נציגי הרשויות ומומחים שונים וכן הובאו בפניה חוות דעת כתובות. בהחלטתה מיום 11.12.14 קבעה הוועדה כי נחה דעתה ביחס לשאלת ההשפעה של המעבר בין המערכות על תוצאות תקופת המבחן כאשר

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נמצא כי לא צפוי הבדל משמעותי בממצאים שיתקבלו בין שתי המערכות, וכי אם יהיה הבדל כזה הוא יהיה זניח ולא ישפיע על תוצאות תקופת המבחן¹.

נושא זה החזר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

5.1.3. אבטחת איכות מסמכים:

מכיוון שמערכת "להב" לא נבנתה מראש כמערכת "סופית" שתשמש את רשות ב' לאורך זמן, נושא כתיבת נהלי אבטחת איכות לא עמד ברמה הנדרשת. רשות ב' התבקשה לערוך את המסמכים כך שיישקפו רמה נדרשת, להטמיע את נהלי הבטחת האיכות ולהתנהל על פיהם. רשות ב' מסרה שהיא נערכת לעריכת המסמכים ולהטמעת הנהלים כמבוקש.

בנושא זה קיים עדיין פער.

5.1.4. בדיקת החלופות:

סעיף 8א (א) בצו מונה שבעה "אופני בדיקות זיהוי" (להלן - "חלופות"/"חלופה") וכן סעיף נוסף, ס"ק 8, המאפשר הוספת אופני בדיקות זיהוי נוספים על ידי הממונה או הוועדה המייעצת. חלופה (1) היא חלופת התשאול אשר אינה כוללת מאגר ביומטרי; חלופות (2-7) הן חלופות הכוללות מאגר, כאשר הן נבדלות אחת מהשנייה בתמהילים שונים של האמצעים או הנתונים הביومترיים; כמו כן, בהתאם לס"ק 8, התווספה חלופה נוספת, על פי הוראת הממונה, היא "שיטת ההקבצים" אשר מהותה היא אחסון נתונים שונה במאגר הביומטרי (ראו להלן). לצורך הליך הפיקוח בנוגע לבדיקת החלופות הועברו אל יחידת הממונה ונבחנו על ידי מכלול המסמכים שנערכו על ידי הרשויות לאורך התקופה, ממצאי הבדיקות המלאים שבוצעו על ידן (לרבות דו"חות מסווגים שהוכנו על ידי מחצ"ב רפא"ל עבור רשות ב', לבדיקות ותהליכי ההשוואות שבוצעו על ידיה) וכן נערכו דיונים עם הרשויות, בראשות הממונה ובמסגרת דיוני הוועדה המייעצת. להלן ייתן פירוט ביחס לנושא בדיקת החלופות וממצאי הליך הפיקוח שנעשה לגביהן.

5.1.5. חלופת התשאול:

חלופת התשאול הינה, כאמור, החלופה היחידה, אשר אינה כוללת מאגר ביומטרי מכל סוג שהוא. רשות א' נערכה לבדיקת החלופה באמצעות ניסוי שיכלול שימוש במתחזים שינסו לצלוח תשאול ולהביא לאישור בקשה להנפקת תיעוד שלא בזהותם האמיתית, בהתאם לנדרש בצו. לנוכח עמדתו של הסטטיסטיקן הממשלתי, שאמור היה לנתח את תוצאות הבדיקה, לפיה ניסוי המבוסס על התחזיות אינו מתאים ולא ניתן יהיה לגזור מתוצאותיו מסקנות בעלת תקפות סטטיסטית, נבדקה השיטה באמצעות מודל הסתברותי שנבנה על ידי הלמ"ס ורשות א', בהתבסס על נתוני תשאול אמיתיים שנאגרו במערכת.

הוועדה המייעצת דנה בנושא זה, וכן הוצגו בפניה המודלים לבדיקת החלופה בפירוט. הוועדה קבעה כי מודל הבדיקה שהוצע על ידי הסטטיסטיקן הממשלתי הוא סביר ונתנה הנחיות נוספות ביחס לבדיקות שיש לבצע. התהליכים הנדרשים שהצביעה עליהם הוועדה המייעצת בוצעו והם מוצגים בפירוט בדו"ח רשות א'. דו"ח רשות א' מציג גם את ממצאי הבדיקה, אשר הצביעו על קשיים ממשיים בהשענות על "חלופת התשאול" ככלי יחיד למניעת "הרכשות כפולות". יצוין כי הוועדה המייעצת (והממונה) קיבלה מסקנה זו של רשות א'².

¹ ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

² ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נושא גיבוש אופן בדיקת חלופת התשאל מוזכר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

במסגרת פעולות הפיקוח שבוצעו בנושא זה, הצביעו הממונה והוועדה המייעצת על הצורך בתיקון סעיף 8 לצו אשר לפיו נדרשות לביצוע בתקופת המבחן "בדיקות יזומות לניסיונות התחזות בזהות כפולה..." לצורך בחינת חלופת התשאל על פי המודל ההסתברותי.

נוסח לתיקון הצו הוצג לוועדה המייעצת במסגרת דיוניה, אולם תיקון זה טרם נעשה.

תגובת רשות א': "לאחר קיום התייעצות במשרד המשפטים הוחלט ברשות האוכלוסין עוד בשלהי שנת 2014, לתקן את סעיף 8 לצו לאור הצורך בשינוי שיטת בדיקת חלופת התשאל. גובש נוסח לתיקון הצו והוא הועבר למשרדי המשפטים והאוצר לצורך קיום חובת התייעצות כנדרש בחוק.

ואולם, נוכח פיזור הכנסת והקדמת הבחירות לא ניתן היה לסיים את התהליך. אנו נדרשים לקבל אישור על קיום חובת התייעצות משרי המשפטים והאוצר ולאחר מכן יידרש אישור ועדת הכנסת המשותפת. הנושא מצוי בטיפול בלשכת השר."

5.1.6. חלופת שיטת ההקבצים:

שיטת ההקבצים הוצעה על ידי פרופ' עדי שמיר ממכון ויצמן כחלופה למבנה המאגר הביומטרי המוגדר בחוק, במטרה "לטשטש" את הקשר החד-ערכי בין זהות אדם לבין הרשומה הביומטרית שלו, ובכך להפחית שימושים משניים שיעשו במאגר הביומטרי. זאת מבלי לפגוע ביעוד העיקרי שלו – מניעת הרכשות כפולות.

בתום הליך לימוד והיוועצות אשר כלל גם פגישות עם הפרופ' שמיר, הורה הממונה בהתאם לסמכותו על פי סעיף 8א(8) לצו, על בדיקתה של השיטה כאחת החלופות. עדכון בנושא זה נמסר לוועדת הכנסת המשותפת ביום 25.4.13.

בוצעה עבודה להפיכת הרעיון לשיטה ברת בדיקה והשיטה המוצעת נבדקה. ממצאי הבדיקה המפורטים בדו"ח רשות ב' הצביעו על קשיים ביכולת ליישם שיטה זו באופן המשיג את מטרותיה, קשיים הנוגעים להיבטים תפעוליים, טכנולוגיים, משפטיים ועוד. יצוין כי הוועדה המייעצת סברה כי ממצאי הבדיקה מצביעים על כך כי חלופת "שיטת ההקבצים" אינה בשלה בעת הזו לצורך מימוש הפרויקט³.

נושא גיבוש אופן בדיקת "שיטת ההקבצים" וביצוע הבדיקה מוזכר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

5.1.7. חלופת 2-7 - חלופת המאגר הביומטרי:

חלופות 2-7 הן החלופות השונות במאגר (טביעת אצבע בודדת, טביעות של שתי אצבעות, תמונת פנים בלבד, תמונה וטביעת אצבע אחת, מאגר מלא ותבניות בלבד).

כאמור, לצורך בחינת החלופות, נמסרו לידי היחידה, מסמכים מפורטים של רשות ב' ושל רפא"ל שפעלה כגוף מקצועי לארגון וניתוח המידע. פירוט ביחס לבדיקת חלופות אלה ובפרט ביחס לחלופת תמונות הפנים ולחלופת התבניות ראו בדו"ח הוועדה המייעצת.

תיקון הבדיקות המוצעות במאגר: סעיף 11(ג) לצו מורה שיש לצרף "חוות דעת של הסטטיסטיקאי הממשלתי בדבר התאמה של הבדיקה והממצאים לכלים המקובלים בתחום זה". בדו"ח המסכם של רשות ב' לא הוצגה חוות הדעת של הסטטיסטיקן הממשלתי, בפרט בנושא חלופות המאגר, ועל כן הורה הממונה לרשות ב' **להציגה ללא דיחוי ולצרפה לדו"ח המסכם.**

בנושא זה קיים פער.

³ראו פירוש נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

5.1.8. קביעת שיטת מתן הציונים לחלופות השונות לפי נושאי הבחינה :

אופני הזיהוי (החלופות) ונושאי הבדיקה (התבחינים, הקריטריונים), נקבעו במסגרת הצו ואופיינו בפרוטוקול.

לאחר תהליך היועצות עם הרשויות, נקבעו המשקלים של כל אחד מהנושאים הנבדקים ואושרו על ידי הוועדה המייעצת.

הרשויות פעלו לקביעת תכולה מדויקת של כל נושא בחינה ולהגדרת אופן קביעת הציונים, תוך היועצות עם הוועדה המייעצת וכן תוך קיום דיונים ישירים בין הממונה לבין הרשויות.

5.1.9. בדיקת נושא החלפת סורקי טביעת אצבע בלשכות והשלכות ההחלפה על איכות ההרכשה :

הרכשת טביעות האצבע לצורך שמירתן בתיעוד ובמאגר הביومتر, מתבצעת באמצעות סורקים אופטיים המותקנים בעמדות ההרכשה ברשות א'. בשל בעיות איכות בסורקים המקוריים שנרכשו, החליפה רשות א' את הסורקים במהלך תקופת המבחן. להחלפת הסורקים כמה משמעותיות והשלכות, כמפורט להלן.

1. **משמעות אחת** נוגעת להיבט הפונקציונאלי. הסוגיה המרכזית היא השאלה - האם יש צורך בהרכשה חוזרת של נתוני התושבים אשר נתונים הורכשו באמצעות הסורקים הישנים. בנושא זה נמסר ליחידת הממונה ע"י הרשויות כי לא יהיה צורך בהרכשה חוזרת.

2. **משמעות שנייה** נוגעת לבקשה של רשות א' לאפשר קבלה של רמת איכות NFIQ3 בהרכשת טביעות האצבע בסורקים החדשים מסיבות תפעוליות בעוד שהצו מורה על קבלת רמות 1 ו-2 בלבד. בנסיבות אלו הבהיר הממונה לרשויות את: א. החובה לפעול לתיקון סעיף 10(ה) לצו. ב. החובה לוודא שחריגה מהגדרות הצו והפרוטוקול, כפי שאושרו במקור, אין בהם כדי לפגוע באיכות ההזדהות מול המאגר, ומול מערכות כמו - משטרת ישראל וביקורת הגבולות במדינת ישראל. לשם כך סבר הממונה, כי עליהן לתאם את ההחלטה עם כל הגורמים הנוגעים בדבר.

נושא זה מצוי בפער וימשיך להימצא במעקב של יחידת הממונה עד לסגירתו.

תגובת רשות א': "בעמדות הביومترיות במערך ביקורת גבולות לא הוחלפו סורקי טביעות האצבע, ולמעשה משתמשים בסורקים מולטי ספקטראליים. חשוב לציין כי נמצא שביצועי האימות של דרכונים שהורכשו עם הסורק החדש (אופטי) מול טביעת אצבע הניטלת במעבר עם סורק מולטי ספקטראלי, טובים יותר מדרכונים שהורכשו עם סורק מולטי ספקטראלי (הישן) והם קרובים לביצועים המוצהרים על ידי היצרן. מבחינת ביקורת הגבולות אין צורך להרכיש מחדש טביעות אצבע שהורכשו עם סורקים מולטי ספקטראליים, שכן המערכת עושה שימוש גם בביומטרית פנים לאימות העובר, כך שהביצועים המשולבים נותנים תוצאות משביעות רצון."

"התיקון המוצע כולל גם תיקון סעיף 10(ה) לצו".

3. **משמעות שלישית**, נוגעת לבדיקת החלופות בתקופת המבחן, ובפרט ביחס לחלופות הכוללות טביעות אצבע, השאלה היא - האם עלול להיות שוני בין התוצאות שיתקבלו בבדיקה של נתונים שהורכשו בסורקים הישנים לעומת בדיקה של נתונים שהורכשו בסורקים החדשים. רשות ב' ומומחים מטעמה הציגו לממונה ולוועדה המייעצת מסמכים ונתונים אשר הבהירו כי בידי רשות ב' היכולת להציג את ההמלצות הסופיות בהסתמך על נתוני הסורקים החדשים, בהיקף נתונים שניתן לתקפו סטטיסטית.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נושא המעבר לסורקים החדשים והשלכות מעבר זה מוזכר בדו"ח המבקר. במועד כתיבת דו"ח זה, השלכת המעבר לסורקים החדשים ביחס לממצאי תקופת המבחן ולהחלטה לגבי המאגר הביומטרי נבדקה ואינה מצויה בפער. הפער שנוצר בנושא זה הינו ביחס לתיאום מול המשטרה ובנושא ההשוואה מול התיעוד, אשר מצוי בבדיקה ומעקב, כאמור בסעיף 5.5 להלן.

5.1.10. בדיקת תקופת המבחן בנתב"ג:

מערכת בקרת הגבולות האוטומטית בנתב"ג (ABC)⁴, החלה לפעול במהלך תקופת המבחן. במערכת זו מבוצעת השוואה בין הנתונים הביומטריים שניטלים מהאדם ובין הנתונים הביומטריים במסמך הזיהוי שלו (מסמכי נסיעה).

בנושא מערכת ה-ABC התמקד הפיקוח של יחידת הממונה בשני עניינים: אבטחת המידע, והיכולת לכייל/לכוון את המערכת.

בנושא אבטחת המידע - המערכת נבדקה על ידי החטיבה ועומדת בדרישותיה. בנושא כיול המערכת - יחידת הממונה סברה שאין להסתמך על המלצות היצרן ויש לבצע ללא דיחוי את בדיקת קצב קבלה מוטעית FAR בשיטת בחינה ומדידה מוכרת וידועה. מימוש הבדיקה ע"י רשות א' חייב את רשות א': א. – לגבש את אופן ביצוע הבדיקה, ו-ב. – קבלת חו"ד משפטית באשר להתאמת הבדיקה להוראות החוק. שני נושאים אלו סוכמו ורשות א' נערכת לביצוע בדיקה עיתית של ה-FAR במעבר.

5.1.11. בדיקת תקופת המבחן במשטרת ישראל:

מתחילת ההערכות לתקופת המבחן מוסדו ממשקי עבודה בין משטרת ישראל לממונה על היישומים הביומטריים. משטרת ישראל הגדירה איש קשר מטעמה לפרויקט בתקופת המבחן – סני"צ מאיר ברקוביץ, הנמצא בקשר רצוף עם היחידה ומרכז את עמדות המשטרה בנושאים השונים שעלו בעת ההכנות לתקופת המבחן ובמהלכה.

הנושאים שהמשטרה נתנה את חוות דעתה היו בין השאר: הגדרת איומי הייחוס, צרכי המשטרה בפרויקט, ממשקים בין המשטרה לרשויות, סימולציות מול המאגר, שיטת ההקבצים, בחירת הסורקים, קבלת רמת איכות NFIQ3, ניקוד החלופות, נחיצות המאגר ותכולתו, חלופת הפנים, תוצאות השוואת אדם מול תעודתו במשטרה, ועוד.

5.2. נושאי אבטחת מידע

נושאי אבטחת מידע בפרויקט מסווגים ברמת סיווג סודי ומפורטים בנספח ב'. הגורם המנחה בנושא אבטחת המידע בפרויקט היא החטיבה לסיכול איומי סייבר.

נכון לכתיבת דו"ח זה לא ידוע על כל חשש קונקרטי להתממשות סיכון דליפת המאגר.

⁴ ABC – Automatic Border Control (מעבר גבול ממוכן על סמך הדרכון הביומטרי ללא בקר גבול אנושי)



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

5.3. נושאי הגנת הפרטיות ברשות א'

5.3.1. מינוי אחראי לנושא הגנת הפרטיות: בעקבות דרישת הממונה ורמו"ט, האחראי מונה ומימש שורת פעילויות בתחום אחריותו, לרבות ביצוע הדרכות וגיבוש נהלים מתאימים.

5.3.2. נוהל הרשאות גישה: הוסדר

5.3.3. גישה למידע מקדים:

במסגרת דו"חות הפיקוח ניתנה התייחסות להנגשת המידע הרלוונטי לציבור בעת ההגעה ללשכות האוכלוסין לקבלת תיעוד, ובטרם ההצטרפות לתקופת המבחן וקבלת תיעוד ביומטרי.

5.3.4. סקר סיכונים:

סקרי הסיכונים שבוצעו ברשות א' בחנו ובדקו גם היבטי אבטחת מידע וגם היבטי פרטיות (בהתאם לתכנית העבודה שקבעה רשות א' עבור עורכי הסקר).

תגובת רשות א': "במסגרת סקר הסיכונים נעשתה הבחנה ברורה בין נושאי אבטחת מידע לנושא הפרטיות. כראיה לכך, בוצע תהליך שלם ומקיף (כרבע משעות הביקורת שהוקצו בסה"כ לסקר) על מנת לבחון את יכולת הפגיעה בפרטיות האזרחים על ידי עובד מרכז ההנפקה.

במהלך הבדיקות, התבקשו אנשי החברה המבצעת את הסקר לנסות ולחדור לרשת מרכז ההנפקה במטרה לצפות או לשנות נתונים תחת הרשאות עובד בלבד (הרשאות נמוכות), כאשר מטרתם העיקרית היתה הגעה לנתונים על מנת לצפות בהם או לשנותם. לאור האמור, במהלך הסקר נעשתה בדיקה מקיפה לנושא יכולות העובד הפשוט לפגוע בפרטיות הנתונים במרכז ההנפקה."

5.3.5. מדיניות אבטחת מידע, הגנת הסייבר וההגנה על הפרטיות:

מסמך המדיניות הועבר ליחידת הממונה. התייחסות בנספח ב'.

5.4. נושאי הגנת הפרטיות ברשות ב'

5.4.1. פעילות הממונה על הפרטיות ברשות:

דו"ח הממונה על הפרטיות הוגש ביום 13.8.14 בהתאם לסעיף 33(ה) לחוק והועבר לגורמים הרלוונטיים המנויים בסעיף זה, לרבות רשם מאגרי המידע ברמו"ט. הדו"ח מפרט את עיקר פעילותו של הממונה על הפרטיות בשנה החולפת. הממונה על הפרטיות עדכן כי הדו"ח השנתי מטעמו יוגש באוגוסט 2015, בהתאם לנדרש בחוק.

5.4.2. תכנית העבודה השנתית להיבטי הפרטיות וסקר סיכונים:

בדו"חות קודמים פורטו מסמכים אשר הוגשו לבקשת יחידת הממונה ובהם תכנית עבודה שנתית המתייחסת להיבטי פרטיות ומסמך איום ייחוס להיבטים אלה, מסמכים המתייחסים למימוש סעיף 25(3) לחוק (Privacy By Design), וכן נהלים נוספים העוסקים בתהליכי העבודה ברשות והנוגעים להיבטי פרטיות. הממונה על הפרטיות העביר תכנית עבודה לשנת 2015.

5.4.3. תפקידו של הממונה על הפרטיות ותפקידים נוספים המוטלים עליו:

בעקבות ההערה שניתנה בדו"חות קודמים לבחינת היחס בין תפקידו של הממונה על הפרטיות לתפקידיו האחרים, פעלו הלשכה המשפטית של משרד הפנים ורשות ב' לגיבוש הסדר מתאים. התייחסות לנושא זה הופיעה בדו"ח פיקוח 2.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

5.4.4. הרשאות הגישה למערכות המחשוב (הזדהות משולשת):

הגישה למערכות המחשוב כנדרש בתקנה 14(ד) נבדקה על ידי יחידת הממונה. מערך הגישה הודגם בעת ביקור ברשות ב' לקראת הוצאת דו"ח פיקוח 2 ונמצא כי היא תואמת לתקנה הנ"ל.

5.4.5. תקנות הממונה על הפרטיות:

הממונה על הפרטיות עדכן כי נוסח תקנות הנוגעות לביצוע תפקידו, מצוי בעבודה משפטית. טיוטת התקנות הועברה ליחידת הממונה.

5.5. פערים ופעילויות שלא הסתיימו בעת הגשת הדו"ח:5.5.1. פערים - רשות א'

5.5.1.1. איכות הרכשת טביעות האצבע NFIQ3 – תאום מול המשטרה

5.5.1.2. תיקון הצו בנושאי NFIQ3 ובדיקת התחזויות

5.5.2. פעילויות נמשכות של רשות א' בעת כתיבת דו"ח זה

5.5.2.1. בנושא אבטחת מידע (נספח ב')

5.5.2.2. בדיקת FAR ברשב"ג

5.5.3. פערים - רשות ב'

5.5.3.1. נהלי אבטחת איכות ועבודה בהתאם לנהלים אלו

5.5.3.2. הצגת חוות דעת של הסטטיסטיקן הראשי בנושא תיקוף בדיקת החלופות במאגר.

5.5.4. פעילויות נמשכות של רשות ב' בעת כתיבת דו"ח זה

5.5.4.1. בדיקות יזומות מול המשטרה לפי סעיף 8(ג) לצו

5.5.5. כללי בפרויקט - אישור (נספח ב')

במהלך תקופת המבחן חלה מגמה ברורה של סגירת פערים. אם בדו"ח הפיקוח מס' 1 סומנו קרוב ל-40 פערים בפרויקט בשתי הרשויות, הרי נכון למועד דו"ח מסכם זה, קיימים פערים בודדים בלבד כמפורט למעלה וכולם מצויים בעבודה. הח"מ מוצא להבהיר כי הפערים הקיימים אינם מונעים התקדמות בפרויקט התעוד הלאומי החכם.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

6. המלצות הממונה לסיום תקופת המבחן

המלצות הוועדה המייעצת מקובלות במלואן על הממונה, הן מובאות בדו"ח המסכם של הוועדה המייעצת שבסימוכין מס' 4 ותמציתן בעמ' 7 שם:

- אין מקום להאריך את תקופת המבחן⁵
- קיימים נימוקים המבססים את נחיצות מאגר המידע הביומטרי
- מאגר המידע הביומטרי יכיל תמונות פנים בלבד ללא טביעות אצבע
- המלצות נוספות לאורך חייו של הפרויקט.

בברכה,

רם ולצר

הממונה על היישומים הביومترיים

העתקים:

מר אלי גרונר – מנכ"ל משרד ראש הממשלה
 מר דוד שרן – מנהל לשכת ראש הממשלה
 עו"ד אלון בכר – ראש הרשות למשפט, מידע וטכנולוגיה, משרד המשפטים
 ראש החטיבה לסיכול איומי הסייבר, משרד ראש הממשלה
 פרופ' דני פפרמן – הסטטיסטיקאי הממשלתי, הלשכה המרכזית לסטטיסטיקה
 עו"ד שלומית ברנע-פרגו – יועמ"ש משרד ראש הממשלה
 מר אבי חליבה – משנה למנכ"ל משרד הפנים
 עו"ד יהודה זימרת – יועמ"ש משרד הפנים
 עו"ד דניאל סלומון – יועמ"ש רשות האוכלוסין וההגירה
 עו"ד אביטל שטרנברג – ראש תחום יעוץ, מחלקת יעוץ וחקיקה, משרד המשפטים
 מר ברוך דדון – מנהל תקופת המבחן, רשות האוכלוסין וההגירה
 מר מאיר גופשטיין – מנהל תקופת המבחן, הרשות לניהול המאגר הביומטרי

⁵הטעון בדיקה – נבדק וניתן לקבל החלטות. אולם לנוכח כניסתו לתפקיד של שר הפנים, סבור הממונה כי יש לאשר את בקשתו של השר ולהאריך את תקופת המבחן. עמדה זו נמסרה ע"י הממונה בדיון ועדת הכנסת המשותפת ביום 24.6.15.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נספחים

בחלק זה ארבעה נספחים:

- נספח א' - ממצאי הפיקוח הכלליים ובתחום הפונקציונאלי של הביומטריה
 נספח ב' - ממצאי הפיקוח בתחום אבטחת המידע – **בסיווג סודי**
 נספח ג' - ממצאי הפיקוח בתחום הגנת הפרטיות וכבוד האדם
 נספח ד' - תגובות הרשויות לטיטות הדו"ח המסכם
 נספח ה' - הנתונים עליהם התבססה המלצת הוועדה המייעצת בנוגע למאגר מבוסס על תמונות פנים בלבד

נספח א' - נושאי הפיקוח וממצאים כלליים ובתחום הפונקציונאלי של הביומטריה

1. נושאים שעליהם יחידת הממונה פיקחה בתקופת המבחן

1.1. תכנית עבודה מפורטת ולוחות זמנים

- 1.1.1. תקופת המבחן הוגדרה בצו למשך שנתיים, כאשר בפועל הנפקת התיעוד ותחילת אגירת המידע במאגר ביום 30.6.13.⁶
- 1.1.2. בתקופת המבחן הוטלו על הרשויות משימות רבות. טרם מתן האישור ליציאה לדרך, התקיים דיון בראשות מנכ"ל משרד ראש הממשלה, ובה העלה הממונה את הדרישה לקיומה של תכנית עבודה מפורטת לקיום הבדיקות והניסויים בתקופת המבחן, והגשתה בתוך 90 יום ממועד תחילת תקופת המבחן.
- 1.1.3. דו"ח הפיקוח הראשון ציין את הצורך בהצגת תכנית עבודה מפורטת, ככלי שנועד לסייע לרשויות להתכנס ללוחות זמנים באופן מסודר, וכדי לוודא את התנהלות התקינה של תקופת המבחן וסיום כל הפעילויות הנדרשות במהלכה.
- 1.1.4. תכנית העבודה המפורטת הוגשה בעיכוב של מספר חודשים, לאחר שהועברו מספר פניות בנושא זה לרשויות. בדו"ח הפיקוח השני צוין כי הפער בנושא זה קיבל מענה, כאשר התכנית הוגשה על ידי הרשויות באופן המאפשר מעקב ועמידה בלוחות זמנים. תכנית העבודה הוצגה בפני הוועדה המייעצת ובפני צוות הפיקוח של יחידת הממונה.

יצוין כי נושא זה הוזכר בדו"ח המבקר ובמועד כתיבת דו"ח פיקוח 2, כבר לא נמצא בו פער.

- 1.1.5. לאחר הצגת תכנית העבודה, העלה הפיקוח מספר נושאים שנראה היה שהם עלולים לגרום לעיכובים בסיום תקופת המבחן במועד, ובהם:
- 1.1.5.1. היערכות בטווח זמן מספק של הלמ"ס, לקבלת נתוני הבדיקות, עיבודם והכללתם בדו"חות התקופתיים הנדרשים ע"פ החוק והצו.
- 1.1.5.2. מימוש בדיקת חלופת התשאול במועד.

⁶ צו המבחן תוקן ביום 23.7.14 וקבע כי תקופת המבחן תחל במועד זה.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

- 1.1.5.3. מימוש בדיקת חלופת ההקבצים במועד.
- 1.1.5.4. מימוש הבדיקות של מערכת ABC בנתב"ג, תוך הצגת התוצאות הנדרשות.
- 1.1.6. החל מאוגוסט 2014, התקבלה תכנית עבודה מפורטת לכל רשות בנפרד. הפיקוח ראה בכך בעיה אפשרית של חוסר אינטגרציה בין שתי תכניות, הקשורות באופן הדוק ביניהן. בהתאם, פנה הממונה למשרד הפנים, עם בקשה שיתבצע תכלול של שתי התכניות, לצורך ראייה כוללת.
- 1.1.7. נושא תכלול תכניות העבודה הוזכר בדו"ח הפיקוח השני אשר ביקש לוודא שיש בידי ועדת ההיגוי של הפרויקט במשרד הפנים תכנית עבודה כוללת של הפרויקט בשתי הרשויות.
- 1.1.8. בנושא זה ציינה רשות א' כי תכניות שתי הרשויות הוצגו בפני ועדת ההיגוי במשרד הפנים. לקראת הגשת הדו"חות המסכמים של הרשויות, נמסר לנו שמר אבי חליבה – סמנכ"ל במשרד הפנים מונה על ידי שר הפנים להיות הגורם המתכלל בפרויקט.
- 1.1.9. לסיכומו של סעיף זה, ייאמר:
- 1.1.9.1. הפיקוח עמד על כך שתוצג תכנית עבודה מפורטת ואינטגרטיבית, שתוודא עמידה בתכולת משימות תקופת המבחן. תכנית זו הוגשה והוצגה לממונה ולוועדה המייעצת.
- 1.1.9.2. היה רצוי כי תכנית העבודה המפורטת הייתה מוגשת בשלב מוקדם יותר של הפרויקט. בסיכומם של דברים, העיכוב בהגשת תכנית העבודה המפורטת לא פגע ביכולת הפיקוח של הממונה ולא מנע את הגשת הדו"חות המפורטים לממצאי תקופת המבחן, בנושאים העיקריים שנדרשו מן הרשויות לצורך גיבוש ההחלטה הנוגעת למאגר הביומטרי.

1.2. תקופת ממצאי תקופת המבחן בהתבסס על מערכת הביניים "להב"

- 1.2.1. תקופת המבחן החלה על גבי מערכת זמנית "להב" (נקראה במקור PLAN B). מתחילה תוכנן לבצע את תקופת המבחן על גבי מערכת בתצורה סופית "מגן" (נקראה במקור PLAN A).
- 1.2.2. עיכוב במכרז למערכת "מגן" גרם לכך שכל תקופת המבחן התנהלה על גבי מערכת "להב". סוגיה זו טופלה על ידי יחידת הממונה מכמה היבטים:
- 1.2.2.1. האם מערכת "להב" מסוגלת לשאת על גבה את כמות ההרכשות עד עלות מערכת "מגן" לעבודה ביצור, ולייצר נתונים תוצאתיים מספקים לבדיקת החלופות בתקופת המבחן.
- 1.2.2.2. האם תוצאות תקופת המבחן עלולות להיות שונות לאור זאת שבתקופת המבחן תיבדק מערכת "להב" לעומת בדיקה באמצעות מערכת "מגן".
- 1.2.3. בסופה של הבחינה, שוכנעה יחידת הממונה שמערכת "להב" מסוגלת לשאת את כמות ההרכשות הצפויה והפקת נתונים, וכן שהחלטות שיתקבלו על גבי מערכת "להב" יהיו תקפות עבור תקופת המבחן וזאת לאחר שהתקבלו מסמכים והסברים מהיועץ הביומטרי של רשות ב' וממומחי מחצ"ב רפא"ל, ומבדיקת מומחי יחידת הממונה, שבדקו ואישרו קביעה זאת.
- 1.2.4. נושא זה נבדק גם על ידי הוועדה המייעצת לאורך מספר דיונים, בהם הופיעו בפניה נציגי הרשויות ומומחים שונים וכן הובאו בפניה חוות דעת כתובות. בהחלטתה מיום 11.12.14 קבעה הוועדה כי נחה דעתה ביחס לשאלת ההשפעה של המעבר בין המערכות על תוצאות

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

תקופת המבחן כאשר נמצא כי לא צפוי הבדל משמעותי בממצאים שיתקבלו בין שתי המערכות, וכי אם יהיה הבדל כזה הוא יהיה זניח ולא ישפיע על תוצאות תקופת המבחן.⁷

נושא זה הוזכר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

1.3. אבטחת איכות מסמכים:

במהלך תקופת המבחן עדכנה רשות ב' את הממונה כי בכוונתה להותיר את מערכת "להב" פעילה כמערכת גיבוי, בנוסף למערכת "מגן". מכיוון שמערכת "להב" לא נבנתה מראש כמערכת "סופית" שתשמש את רשות ב' לאורך זמן, נושא כתיבת נהלים וההתנהלות על פי נהלים אלו לא עמד ברמה הנדרשת. רשות ב' התבקשה לערוך את המסמכים, להטמיע את נהלי הבטחת האיכות ולהתנהל על פיהם. רשות ב' מסרה שהיא נערכת לעריכת המסמכים ולהטמעת הנהלים כמבוקש.

בנושא זה קיים עדיין פער.**1.4. בדיקת החלופות**

1.4.1. סעיף 8א (א) בצו מונה שבעה "אופני בדיקות זיהוי" (להלן - "חלופות"/"חלופה") וכן סעיף נוסף, ס"ק 8, המאפשר הוספת אופני בדיקות זיהוי נוספים על ידי הממונה או הוועדה המייעצת.

חלופה (1) היא חלופת התשאל אשר אינה כוללת מאגר ביומטרי; חלופות (2-7) הן חלופות הכוללות מאגר, כאשר הן נבדלות אחת מהשנייה בתמהילים שונים של האמצעים או הנתונים הביومترיים; כמו כן, בהתאם לס"ק 8, התווספה חלופה נוספת, על פי הוראת הממונה, היא "שיטת ההקבצים" אשר מהותה היא אחסון נתונים שונה במאגר הביומטרי (ראו להלן).

1.4.2. לצורך הליך הפיקוח בנוגע לבדיקת החלופות הועברו אל יחידת הממונה ונבחנו על ידי מכלול המסמכים שנערכו על ידי הרשויות לאורך התקופה, ממצאי הבדיקות המלאים שבוצעו על ידן (לרבות דו"חות מסווגים שהוכנו על ידי מחצ"ב רפא"ל עבור רשות ב', לבדיקות ותהליכי ההשוואות שבוצעו על ידיה) וכן נערכו דיונים עם הרשויות, בראשות הממונה ובמסגרת דיוני הוועדה המייעצת.

1.4.3. במהלך תקופת המבחן, ניתן דגש מיוחד לצורך בבדיקה שיטתית של כל החלופות, ובפרט אלו שמהוות חלופה למאגר הביומטרי, במתכונתו המלאה. זאת, על מנת להבטיח שנעשה כל הנדרש להביא לידי ביטוי את היתרונות בשיטות החלופיות, כמו גם חסרונותיהן, בצורה מקצועית ואובייקטיבית.

להלן יינתן פירוט ביחס לנושא בדיקת החלופות וממצאי הליך הפיקוח שנעשה לגביהן.

1.4.4. חלופת התשאל:

1.4.4.1. חלופת התשאל הינה החלופה היחידה, מבין החלופות אשר הצו קובע כי יבחנו בתקופת המבחן, אשר אינה כוללת מאגר ביומטרי מכל סוג שהוא.

1.4.4.2. סעיף 8א(א)(1) לצו קובע כי בדיקת חלופת התשאל תעשה במתווה שנקבע להליך התשאל הננקט בלשכות האוכלוסין בתקופת המבחן על פי התקנות תוך שימוש בכלל האמצעים שניתן לנקוט לווידוא ואימות זהות לפי תקנות אלה.

1.4.4.3. רשות א' נערכה לבדיקת החלופה באמצעות ניסוי שיכלול שימוש במתחזים שינסו לצלוח תשאל ולהביא לאישור בקשה להנפקת תיעוד שלא בזהותם האמיתית,

⁷ ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

בהתאם לנדרש בצו. שיטה זאת דרשה היערכות מתאימה של רשות א', והרשות נערכה למימושה

1.4.4.4. לנוכח עמדתו של הסטטיסטיקן הממשלתי, שאמור היה לנתח את תוצאות הבדיקה, לפיה ניסוי המבוסס על התחזיות אינו מתאים ולא ניתן יהיה לגזור מתוצאותיו מסקנות בעלת תקפות סטטיסטית, נבדקה השיטה באמצעות מודל הסתברותי שנבנה על ידי הלמ"ס ורשות א', בהתבסס על נתוני תשאול אמיתיים שנאגרו במערכת.

1.4.4.5. הוועדה המייעצת דנה בנושא זה, וכן הוצגו בפניה המודלים לבדיקת החלופה בפירוט. הוועדה קבעה כי מודל הבדיקה שהוצע על ידי הסטטיסטיקן הממשלתי הוא סביר ונתנה הנחיות נוספות ביחס לבדיקות שיש לבצע. התהליכים הנדרשים שהצביעה עליהם הוועדה המייעצת בוצעו והם מוצגים בפירוט בדו"ח רשות א'.

1.4.4.6. תוצאות הבדיקה המוצגים בדו"ח רשות א', הראו שבעוד שהסיכוי של אדם תמים לעבור את ההליך הוא 80%, הרי שמתחזים כדוגמת שוהה בלתי חוקי וארגוני פשיעה, טרור וריגול עלולים לעבור את ההליך בהסתברויות גבוהות יותר. מכאן נגזרה המסקנה שחלופת התשאול אינה עומדת במדדים שנקבעו בצו, של 95% מניעת הרכשה כפולה.

1.4.4.7. נבדקה אפשרות להגדיר "תשאול מוגבר" שיעמוד בדרישות הצו למנוע הרכשה כפולה של 95% מהמתחזים. אולם נמצא כי מחיר הקשחת התהליך יביא לכך שהסיכוי שתושב "תמים" יוכל לעבור את התשאול, ירד. כלומר, שרוב התושבים "התמימים" ייכשלו בקו הראשון ויצטרכו לעבור לתחקיר בקו שני, דבר שאינו ראוי מבחינה תפעולית.

1.4.4.8. דו"ח רשות א' הצביע על קשיים ממשיים בהשענות על "חלופת התשאול" ככלי יחיד למניעת "הרכשות כפולות". רשות א' העלתה שורה של נימוקים נוספים למסקנה לפיה לא ניתן להישען על חלופת התשאול ככלי יחיד, כאמור, ובהם היכולת המוגבלת בתקנות לביצוע תשאול עומק והאיסור לשימוש במידע רגיש וכן ההערכה לפיה לא ניתן יהיה למנוע את פרסום השאלות לאורך זמן.

1.4.4.9. הוועדה המייעצת והממונה קיבלו מסקנה זו של רשות א'.⁸

נושא גיבוש אופן בדיקת חלופת התשאול מוזכר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

1.4.4.10. במסגרת פעולות הפיקוח שבוצעו בנושא זה, הצביעו הממונה והוועדה המייעצת על הצורך בתיקון סעיף 38 לצו אשר לפיו נדרשות לביצוע בתקופת המבחן "בדיקות יזומות לניסיונות התחזות בזהות כפולה..." לצורך בחינת חלופת התשאול על פי המודל ההסתברותי.

נוסח לתיקון הצו הוצג לוועדה המייעצת במסגרת דיוניה, אולם תיקון זה טרם נעשה.

תגובת רשות א': "לאחר קיום התייעצות במשרד המשפטים הוחלט ברשות האוכלוסין עוד בשלהי שנת 2014, לתקן את סעיף 38 לצו לאור הצורך בשינוי שיטת בדיקת חלופת התשאול. גובש נוסח לתיקון הצו והוא הועבר למשרדי המשפטים והאוצר לצורך קיום חובת התייעצות כנדרש בחוק.

⁸ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219

הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

ואולם, נוכח פיזור הכנסת והקדמת הבחירות לא ניתן היה לסיים את התהליך. אנו נדרשים לקבל אישור על קיום חובת התייעצות משרי המשפטים והאוצר ולאחר מכן יידרש אישור ועדת הכנסת המשותפת. הנושא מצוי בטיפול בלשכת השר."

1.4.5. חלופת שיטת ההקבצים:

1.4.5.1. שיטת ההקבצים הוצעה על ידי פרופ' עדי שמיר ממכון ויצמן כחלופה למבנה המאגר הביומטרי המוגדר בחוק, במטרה להפחית במידה ניכרת ("לטשטש") את הקשר החד-ערכי בין זהות אדם לבין הרשומה הביומטרית שלו, ובכך להפחית שימושים משניים שיעשו במאגר הביומטרי. זאת מבלי לפגוע בייעוד העיקרי שלו – מניעת הרכשות כפולות.

1.4.5.2. בתום הליך לימוד והיוועצות אשר כלל גם פגישות עם הפרופ' שמיר, הורה הממונה בהתאם לסמכותו על פי סעיף 8א(8) לצו, על בדיקתה של השיטה כאחת החלופות. עדכון בנושא זה נמסר לוועדת הכנסת המשותפת ביום 25.4.13.

1.4.5.3. בנוסף, לכך, נעשתה עבודה על ידי יחידת הממונה לכתיבת מסמך אב להגדרתה של "שיטת ההקבצים", לצורך בדיקה. גיבוש מסמך זה נעשה בתיאום עם פרופ' עדי שמיר עצמו והוא נשלח לרשות ב' לשם גיבוש תכנית הניסוי על ידה.

1.4.5.4. במסגרת תכנית העבודה, תכננה רשות ב' לבדוק את שיטת ההקבצים על מערכת "מגן". אולם, משהתברר שמערכת "מגן" לא תהיה מוכנה במהלך תקופת המבחן, החליטה רשות ב' להיערך לבדיקת השיטה על גבי מערכת "להב". לצורך כך ערכה רשות ב' את מסמכי האפיון והבדיקות כנדרש בפרט על בסיס התייעצות עם פרופ' שמיר על אופן המימוש של השיטה.

1.4.5.5. ממצאי הבדיקה המפורטים בדו"ח רשות ב' הצביעו על קשיים ביכולת ליישם שיטה זו באופן המשיג את מטרותיה, קשיים הנוגעים להיבטים תפעוליים, טכנולוגיים, משפטיים ועוד. יצוין כי הוועדה המייעצת סברה כי ממצאי הבדיקה מצביעים על כך כי חלופת "שיטת ההקבצים" אינה בשלה בעת הזו לצורך מימוש הפרויקט⁹.

נושא גיבוש אופן בדיקת "שיטת ההקבצים" וביצוע הבדיקה מוזכר בדו"ח המבקר ובמועד כתיבת דו"ח זה, לא מצוי בו פער.

1.4.6. חלופות 2-7 - חלופות המאגר הביומטרי:

1.4.6.1. חלופות 2-7 הן החלופות השונות במאגר (טביעת אצבע בודדת, טביעות של שתי אצבעות, תמונת פנים בלבד, תמונה וטביעת אצבע אחת, מאגר מלא ותבניות בלבד).

1.4.6.2. בדו"ח פיקוח מס' 2 העירה יחידת הממונה על כך שחסר מסמך תכנון בדיקות ומסמך ביצוע בדיקות המאגדים את הנושא בצורה ראויה. המסמכים המבוקשים הוכנו והוגשו.

1.4.6.3. לצורך בחינת החלופות, הועברו ליחידה מסמכים מפורטים של רשות ב' ושל רפ"ל שפעלה כגוף מקצועי לארגון וניתוח המידע.

1.4.6.4. בהקשר זה יש לציין כי הציונים שניתנו לחלופת הפנים בלבד, לא הסתמכו על נתוני הבדיקות שבוצעו במאגר ונותחו ע"י רפ"ל. הסיבה לכך היא הפרש הזמנים הקצר שעבר בין ההרכשה הראשונית לנטילת תמונות נוספת של האוכלוסייה שחידשה את התייעוד או שביקשה תיעוד נוסף במהלך תקופת המבחן. כתחליף רשות ב' הציבה את

⁹ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219

הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

אחוזי הדיוק שנמסרו על פי הצהרת היצרן. בעניין זה בוצע ניתוח נפרד, הכלול בהמלצות הוועדה המייעצת.

1.4.7. תיקוף הבדיקות המבוצעות במאגר

1.4.7.1. סעיפים 11(ב) ו-11(ג) לצו מורים כי "הרשות לניהול המאגר הביومترית ורשות האוכלוסין יכינו דין וחשבון מפורט בכתב ובו תיאור כל תוצאות הבדיקות שבוצעו בתקופה האמורה בצו... דין וחשבון כאמור יערך לפי כללים מקובלים לעריכת מבדקים למערכות ביומטריות, ככל שהם רלוונטיים, ובכלל זה יסקור את הממצאים והאסמכתאות לממצאים בהתאם לפרוטוקול המבחן, וכן חוות דעת של הסטטיסטיקאי הממשלתי בדבר התאמה של הבדיקה והממצאים לכלים המקובלים בתחום זה".

1.4.7.2. הלשכה המרכזית לסטטיסטיקה ליוותה את תהליכי הבדיקות שנעשו בתקופת המבחן על ידי שתי הרשויות לאורך התקופה כנדרש בצו. כמו כן, הבדיקות שבוצעו על ידי רשות ב' ובמרכזן בדיקת החלופות בהתאם לנדרש בצו, לוותה גם על ידי יחידת מחצ"ב רפ"ל. במסגרת ליווי זה נבדק תיקופם של מכלול ההיבטים של התהליך, כולל איסוף הנתונים, שיטות המדידה, החישובים, הניתוח והסקת המסקנות.

1.4.7.3. לקראת תום תקופת המבחן, מצאו חברי הוועדה המייעצת, ובהם הסטטיסטיקן הממשלתי, כמפורט בדו"ח הוועדה (סימוכין 4), כי "עיקרי הנושאים המרכזיים אשר על בחינתם הורה הצו נבדקו וקיימים נתונים מספקים לשם קבלת החלטה".

1.4.7.4. מכיוון שבדו"ח המסכם של רשות ב' לא הוצגה חוות דעת של הסטטיסטיקן הממשלתי, פנתה יחידת הממונה ב-25.6.15 לרשות ב' וביקשה **להציג את חוות הדעת של הבלמ"ס ללא דיחוי ולצרפה לדו"ח המסכם. בנושא זה קיים פער.**

1.5. קביעת שיטת מתן הציונים לחלופות השונות לפי נושאי הבחינה:

- 1.5.1. חשיבות נושא זה הינה בשימוש בו לצורך דירוג החלופות השונות, כבסיס לקבלת החלטות בתום תקופת המבחן.
- 1.5.2. אופני הזיהוי (החלופות) ונושאי הבדיקה (התבחינים, הקריטריונים), נקבעו במסגרת הצו ואופיינו בפרוטוקול.
- 1.5.3. לאחר תהליך היוועצות עם הרשויות, קבעה הוועדה המייעצת ב-10.11.13 את המשקלים של כל אחד מהנושאים הנבדקים.
- 1.5.4. בהמשך התנהל ברשויות תהליך לקביעת התכולה של כל נושא בחינה והגדרת אופן קביעת הציונים, תוך היוועצות עם הוועדה המייעצת ועם יחידת הממונה, וגיבשה את מסמך "אופן מתן הציונים" בו מתוארת שיטת הניקוד של הנושאים הנבדקים.
- 1.5.5. הוועדה המייעצת קיימה מספר דיונים לגבי מסמך "אופן מתן הציונים" והוגשו לה מספר גרסאות של מסמך זה, במקביל לדיוני ההיוועצות לגבי מתן הציונים המספריים¹⁰.

1.6. בדיקת נושא החלפת סורקי טביעת אצבע בלשכות והשלכות ההחלפה על איכות ההרכשה:

- 1.6.1. איכות נטילת המידע הביومترית, בתהליך ההרכשה, מהווה מרכיב חשוב בכל הקשור ליכולת הגורמים המסתמכים על השימוש במידע זה, לבצע בהצלחה את הזיהוי או האיתות הביומטרי, על פי המדדים שנקבעו בתקנות ובצו.
- 1.6.2. הרכשת טביעות האצבע לצורך שמירתן בתיעוד ובמאגר, מתבצעת באמצעות סורקים אופטיים המותקנים בעמדות ההרכשה בלשכות רשות א'. בשל בעיות איכות בסורקים

¹⁰ ראו פירוט נוסף בדו"ח הוועדה המייעצת מיום 28.5.15

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

- המקוריים שנרכשו, החליפה רשות א' את הסורקים במהלך תקופת המבחן. להחלפת הסורקים כמה משמעותיות והשלכות, כמפורט להלן.
- 1.6.2.1. **משמעות אחת** נוגעת להיבט הפונקציונאלי. הסוגיה המרכזית היא השאלה - האם יש צורך בהרכשה חוזרת של נתוני התושבים אשר נתונים הורכשו באמצעות הסורקים הישנים. בנושא זה נמסר ליחידת הממונה ע"י רשות א' כי לא יהיה צורך בהרכשה חוזרת.
- 1.6.2.2. **משמעות שנייה** נוגעת לבקשה של רשות א' לאפשר קבלה של רמת איכות NFIQ3 בהרכשת טביעות האצבע בסורקים החדשים מסיבות תפעוליות בעוד שהצו מורה על קבלת רמות 1 ו-2 בלבד.
- 1.6.2.3. בנסיבות אלו הבהיר הממונה לרשויות את: א. החובה לפעול לתיקון סעיף 10(ה) לצו. ב. החובה לוודא שחריגה מהגדרות הצו והפרוטוקול, כפי שאושרו במקור, אין בהם כדי לפגוע באיכות ההזדהות מול המאגר, ומול מערכות כמו - משטרת ישראל וביקורת הגבולות במדינת ישראל. לשם כך סבר הממונה, כי עליהן לתאם את ההחלטה עם כל הגורמים הנוגעים בדבר.
- 1.6.2.4. לעניין הראשון, הודיעה רשות א', כי היא פועלת במישור המשפטי, לתיקון סעיף 10(ה) לצו.
- 1.6.2.5. מול רשות ב' ורשב"ג התאום בוצע. באשר למשטרה, ב-12.4.15 הועברה התייחסות של סני"צ דוד אטיאס ראש מעבדת ט"א במז"פ, בנושא ובסיכום נאמר: "משטרת ישראל מתנגדת למעבר משימוש באיכות ברמה 1-2, כפי שמתחייב מן הצו, לשימוש גם באיכות ברמה 3, בעת ההרכשה".
- 1.6.2.6. ב-19.4.15 פנה הממונה לרשות האוכלוסין וההגירה וביקש שרשות האוכלוסין תיזום דיון דחוף עם כל הגורמים הרלוונטיים לנושא על מנת לבחון ולגבש מענה מתואם. הממונה הוסיף והדגיש שהוא סבור שיש להימנע מקבלת הרכשות טביעות אצבע לפי מדד NFIQ3, עד לליבון הסוגיה לרבות הסדרתה המשפטית.
- 1.6.2.7. ב-14.6.15 התקבל עדכון מרשות האוכלוסין ש"נקבעה פגישה עם כל הגורמים הרלוונטיים על מנת ליישר קו בנושא ולהגיע לפתרון מתואם כפי שכתבת".

נושא זה מצוי בפער וימשיך להימצא במעקב של יחידת הממונה עד לסגירתו.

תגובת רשות א': "בעמדות הביומטריות במערך ביקורת גבולות לא הוחלפו סורקי טביעות האצבע, ולמעשה משתמשים בסורקים מולטי ספקטראליים. חשוב לציין כי נמצא שביצועי האימות של דרכונים שהורכשו עם הסורק החדש (אופטי) מול טביעת אצבע הניטלת במעבר עם סורק מולטי ספקטראלי, טובים יותר מדרכונים שהורכשו עם סורק מולטי ספקטראלי (הישן) והם קרובים לביצועים המוצהרים על ידי היצרן. מבחינת ביקורת הגבולות אין צורך להרכיש מחדש טביעות אצבע שהורכשו עם סורקים מולטי ספקטראליים, שכן המערכת עושה שימוש גם בביומטריית פנים לאימות העובר, כך שהביצועים המשולבים נותנים תוצאות משביעות רצון."

"התיקון המוצע כולל גם תיקון סעיף 10(ה) לצו."

- 1.6.2.8. **משמעות שלישית**, נוגעת לבדיקת החלופות בתקופת המבחן, ובפרט ביחס לחלופות הכוללות טביעות אצבע, השאלה היא - האם עלול להיות שוני בין התוצאות שיתקבלו בבדיקה על גבי נתונים שהורכשו בסורקים הישנים לעומת בדיקה על גבי

כתובת לקבלת דואר: קפולן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נתונים שהורכשו בסורקים החדשים. הנושא נדון במסמכים של מחצ"ב/רפא"ל שהוגשו על ידי רשות ב'. במסמכים אלו נבדקת העמידה בסף הנדרש, של סורק טביעת האצבע החדש עבור אימות וזיהוי על פי אצבע אחת ושתי אצבעות והיתוך של שתי אצבעות ופנים. רשות ב' ומומחים מטעמה הציגו לממונה ולוועדה המייעצת בישיבתה ביום 11.12.2014 מסמכים ונתונים אשר הבהירו כי בידי רשות ב' היכולת להציג את ההמלצות הסופיות בהסתמך על נתוני הסורקים החדשים, באופן שניתן לתקפו סטטיסטית.

נושא המעבר לסורקים החדשים והשלכות מעבר זה מוזכר בדו"ח המבקר. במועד כתיבת דו"ח זה, השלכת המעבר לסורקים החדשים ביחס לממצאי תקופת המבחן ולהחלטה לגבי המאגר הביומטרי נבדקה ואינה מצויה בפער.
הפער שנוצר בנושא זה הינו ביחס לתיאום מול המשטרה ובנושא ההשוואה מול התיעוד, אשר מצוי בבדיקה ומעקב, כאמור לעיל ובסעיף 5.5 להלן.

1.7. בדיקת תקופת המבחן בנתב"ג:

- 1.7.1. מערכת בקרת הגבולות האוטומטית בנתב"ג (ABC)¹¹, החלה לפעול במהלך תקופת המבחן. במערכת זו מבוצעת השוואה בין הנתונים הביומטריים שניטלים מהאדם ובין הנתונים הביומטריים במסמך הזיהוי שלו (מסמכי נסיעה).
- 1.7.2. בנושא מערכת ה-ABC התמקד הפיקוח של יחידת הממונה בשני עניינים: אבטחת המידע, והיכולת לכייל/לכוון את המערכת.
- 1.7.3. אבטחת המידע: המערכת נבדקה על ידי החטיבה ועומדת בדרישותיה.
- 1.7.4. בנושא כיול המערכת סברה יחידת הממונה שאין להסתמך על המלצות היצרן בנושא כיול המערכת ויש לבצע ללא דיחוי את בדיקת קצב קבלה מוטעית FAR בשיטת בחינה ומדידה מוכרת וידועה.
- 1.7.5. מימוש הבדיקה ע"י רשות א' חייב: א. – גיבוש אופן ביצוע הבדיקה, ו-ב. – קבלת חו"ד משפטית באשר להתאמת הבדיקה להוראות החוק. שני נושאים אלו סוכמו ורשות א' נערכת לביצוע בדיקת ה-FAR במעבר. נערכת הרשות לבניית מודול תוכנה תואם FRONTEX שיאפשר בדיקה עיתית של ה-FAR במעבר.

1.8. בדיקת תקופת המבחן במשטרת ישראל:

- 1.8.1. מתחילת ההערכות לתקופת המבחן מוסדו ממשקי עבודה בין משטרת ישראל לממונה על היישומים הביומטריים. משטרת ישראל הגדירה איש קשר מטעמה לפרויקט בתקופת המבחן – סני"צ מאיר ברקוביץ הנמצא בקשר רצוף עם היחידה ומרכז את עמדות המשטרה בנושאים השונים שעלו בעת ההכנות לתקופת המבחן ובמהלכה.
- 1.8.2. הנושאים שהמשטרה נתנה את חוות דעתה היו בין השאר: הגדרת איומי הייחוס, צרכי המשטרה בפרויקט, ממשקים בין המשטרה לרשויות, סימולציות מול המאגר, שיטת ההקבצים, בחירת הסורקים, קבלת רמת איכות NFIQ3, ניקוד החלופות, נחיצות המאגר ותכולתו, חלופת הפנים, תוצאות השוואת אדם מול תעודתו במשטרה, ועוד.
- 1.8.3. ב-10.3.14 הועברה למשטרה טיוטה להתייחסות של תכנית הפיקוח של הממונה על היישומים הביומטריים על משטרת ישראל מכוח החוק. לאחרונה התקבלה התייחסות המשטרה לתכנית הפיקוח ונקבעה ישיבת עבודה בנושא.

¹¹ ABC – Automatic Border Control (מעבר גבול ממוכן על סמך הדרכון הביומטרי ללא בקר גבול אנושי)

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

2. הערות לדוחות המסכמים של הרשויות

בסוף מרץ 2015 הפיצו שתי הרשויות דו"חות מסכמים לתקופת המבחן בו הציגו את ממצאי תקופת המבחן.

יחידת הממונה למדה דו"חות אלו ושאלה מספר שאלות, רוב השאלות קיבלו מענה.

השאלה הבאה נמצאת עדיין בבדיקה:

טבלת החרیגים שבסעיף 8.8 בדו"ח המסכם של רשות ב'. בטבלה זו צוינו 617 אירועים חריגים. הממונה ביקש לקבל הבהרה כמה **אירועי התחזות היו וכמה מאירועים אלה מהווים טעויות אנוש או טעויות מסוג אחר**. הממונה העיר כי הצגת הנתונים בדו"ח המסכם של רשות ב' באופן לא מבואר, עלולה לתת בידי הקורא תמונה שאינה מהימנה ומלאה לגבי אירועים אלה וטיבם.

רשות ב' הודיעה שאין בידה את הנתונים המבוקשים, שכן אין בידי רשות ב' פרטים מזהים מעבר למידע הביומטרי, ולכן אירועים אלה הועברו לבדיקת רשות א'.

התייחסות נוספת לדו"חות הרשויות ולמסקנותיהן מופיעה בדו"ח הוועדה המייעצת.

יצוין כי השאלות והתשובות על הדו"חות המסכמים לא שינו את תוצאות הדירוג בין החלופות ואין בהן כדי לשנות מהמלצות הממונה לתום תקופת המבחן.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נספח ג' – הפיקוח בתחום הגנת הפרטיות וכבוד האדם**1. כללי**

- 1.1. סעיף 1 לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשי"ע - 2009 (להלן - החוק), קובע את מטרות החוק, כאשר המטרה השלישית היא- "קביעת ההסדרים הנדרשים לשם הגנת הפרטיות של התושבים שניטל מהם המידע הביומטרי ובכלל זה דרכי הגישה למאגר הביומטרי ואבטחת המידע בו".
- 1.2. נושא אבטחת המידע והגנת הפרטיות הם נושאים השזורים אחד בשני, אולם לשם ההבהרה ניתן לומר כי אמצעי אבטחת מידע שונים נועדו לשמש ככלים לשם הגנת הפרטיות (ועשויים להיות כלים נוספים).
- 1.3. במסגרת תכנית הפיקוח נכתב פרק נפרד ל"הגנת הפרטיות" במובחן מפרק אבטחת המידע.
- 1.4. ממצאי דו"ח פיקוח מס' 3 של הממונה, הדו"ח המסכם, מבוססים על פגישות עם הרשויות וגורמים רלוונטיים נוספים, והמסמכים שהועברו לממונה בהתאם לבקשתו לאורך התקופה. לאורך "תקופת המבחן" נערכו מספר ביקורים באתרי הפרויקט וממצאי הביקורים שמשו לכתיבת דו"חות הפיקוח, לרבות לעניין הגנת הפרטיות.
- 1.5. דו"ח הפיקוח המסכם להיבטי הגנת הפרטיות מבטא "חיתוך מצב" הנכון לחציון הראשון של שנת 2015, כשנתיים לאחר תחילתה של תקופת המבחן ועליית הפרויקט לאוויר.

2. מעקב אחר ממצאים עיקריים:**2.1. רשות האוכלוסין, ההגירה ומעברי הגבול (רשות א')**

להלן התייחסות לעיקרי הממצאים הפרטניים שעלו ביחס לרשות האוכלוסין:

- 2.1.1. מינוי אחראי לנושא הגנת הפרטיות ביחס לפרויקט וטיפול בנושא ההגנה על הפרטיות:
בעקבות הערת הממונה על הצורך במינוי אחראי לנושא הפרטיות ברשות א' במסגרת דו"חות הפיקוח הקודמים, התקבלה החלטה לפיה הממונה על אבטחת המידע ברשות א' ישמש גם כאחראי על הגנת הפרטיות ביחס לפרויקט דן (להלן - "האחראי").
- האחראי פעל להכנת תכנית עבודה שנתית המתייחסת להיבטי פרטיות (הועברה לעיונינו תכנית לשנת 2014 וכן עדכון לשנת 2015), להכנת נוהל ללשכות רשות האוכלוסין המאגד בתוכו את הנחיות החקיקה הנוגעות להגנת הפרטיות וכבוד האדם (לרבות ביחס לאוכלוסיות מיוחדות), תכנית ביקורות בלשכות בהיבטי אבטחת מידע ופרטיות ועוד.
- האחראי מקיים הדרכות שוטפות בלשכות האוכלוסין הכוללות התייחסות להגנת הפרטיות. בהדרכות אלה עובר האחראי עם עובדי הלשכות על תהליכי העבודה הקשורים בפרויקט התייעוד החכם וכן ניתנים דגשים על נושא ההסכמה והחתימה על הטפסים והתייחסות נפרדת לרגישויות בממשק עם אוכלוסיות מיוחדות. האחראי משולב גם בהדרכה המתקיימת לעובדים החדשים של הרשות, להיבטי אבטחת מידע ופרטיות.
- האחראי קיים ביקורים גם באתרים אחרים של רשות א', "ארבל" ו"פתקית" (אתרי הנפקת תיעוד), באתרים אלה התקיימה גם הדרכה של הרשות למשפט טכנולוגיה ומידע לבקשתו של האחראי, בדצמבר 2014 ובינואר 2015.
- בנוסף, קיים האחראי הרצאות גם לדרג הניהול של רשות א'.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

2.1.2. הכשרת עובדים לפי תקנה 15 לתקנות הכללת אמצעי זיהוי ביومترיים

בינואר 2015 תוקנו התקנות שנחקקו מכוח החוק, כך שהתווספה תקנה 15 הקובעת מהם נושאי ההכשרה אשר יועברו למי שניתנה לו סמכות נטילה, הפקה או השוואה לפי פרק ג' לחוק. רשות א' מסרה כי היא מקיימת ימי עיון והכשרה בהתאם לנדרש בתקנה זו, תוך התייחסות לכל התכנים הרלוונטיים. בעניין נושאי הגנת הפרטיות ואבטחת המידע ראו האמור בסעיף 2.1.1 לעיל. נושא זה יהיה מצוי במעקב יחידת הממונה במסגרת תהליכי העבודה השוטפים.

2.1.3. הגדרת הרשאות גישה:

בעקבות הערת הממונה בנושא זה, התקבל נוהל הרשאות למערכת "אביב", ראה התייחסות לנושא בנספח ב' סעיף 4.6.

2.1.4. גישה למידע מקדים:

במסגרת דו"חות הפיקוח קודמים ניתנה התייחסות להנגשת המידע הרלוונטי לציבור בעת ההגעה לשכונת האוכלוסין לקבלת תיעוד, ובטרם ההצטרפות לתקופת המבחן וקבלת תיעוד ביומטרי, במטרה לבחון את יישום הוראות הצו, ובפרט סעיף 3 לצו העוסק בהסכמת התושב. בין היתר צוין בדו"חות כי קיים מידע רב ומפורט הנגיש לציבור באתר האינטרנט של רשות א', כאשר סעיף 3 לצו קובע גם כי על עובד לשכת האוכלוסין למסור לתושב שעשוי להצטרף לתקופת המבחן "דף הסבר" הכולל התייחסות לנושאים מרכזיים בקשר לפרויקט, לרבות הכללת האמצעים והנתונים הביومترיים במאגר ביומטרי.

הערת הממונה בנושא זה, אשר ניתנה לאחר ביקורות שנערכו במספר לשכות, הייתה כי יש צורך לחדד את הנהלים ולרענן את ההדרכה וההכשרה שניתנה לנותני השירות בשכונות. וכי על רשות א' לוודא כי דפי המידע והטפסים יהיו נגישים, בשפות השונות, בכל אחת מהלשכות, באופן המאפשר הזדמנות נאותה לתושבים לקרוא את החומר ולפני קבלת השירות/ביצוע ההרכשה עצמה, ולהקפדה יתרה בנושא זה.

בנושא ריענון הנהלים וההכשרות לנותני השירות בשכונות, פעל האחראי לנושא פרטיות כמתואר בסעיף 2.1.1 לעיל. לעניין הנגשת המידע בשכונות, מסרה רשות א' בעבר כי "בלשכות קיים מידע נגיש לצבור בנושא התיעוד הביומטרי בכמות רבה ומגוונת" וכי "המנהלים והפקידים בשכונות מתודרכים באופן שוטף לוודא ולהקפיד כי דפי המידע והטפסים יהיו נגישים לקהל".

2.1.5. סקר סיכונים:

סקרי הסיכונים שבוצעו ברשות א' בחנו ובדקו גם היבטי אבטחת מידע וגם היבטי פרטיות (בהתאם לתכנית העבודה שקבעה רשות א' עבור עורכי הסקר).

תגובת רשות א': "במסגרת סקר הסיכונים נעשתה הבחנה ברורה בין נושאי אבטחת מידע לנושא הפרטיות. כראיה לכך, בוצע תהליך שלם ומקיף (כרבע משעות הביקורת שהוקצו בסה"כ לסקר) על מנת לבחון את יכולת הפגיעה בפרטיות האזרחים על ידי עובד מרכז ההנפקה.

במהלך הבדיקות, התבקשו אנשי החברה המבצעת את הסקר לנסות ולחדור לרשת מרכז ההנפקה במטרה לצפות או לשנות נתונים תחת הרשאות עובד בלבד (הרשאות נמוכות), כאשר מטרתם העיקרית היתה הגעה לנתונים על מנת לצפות בהם או לשנותם. לאור האמור, במהלך הסקר נעשתה בדיקה מקיפה לנושא יכולות העובד הפשוט לפגוע בפרטיות הנתונים במרכז ההנפקה."

2.1.6. מדיניות אבטחת מידע, הגנת הסייבר וההגנה על הפרטיות ברשות א':

מסמך מדיניות זה הועבר ליחידת הממונה, לגבינו ראו התייחסות בנספח ב' בסעיף 4.5.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

2.2. הרשות לניהול המאגר הביומטרי (רשות ב')

להלן התייחסות לממצאים הפרטניים שעלו ביחס לרשות לניהול המאגר הביומטרי:

2.2.1. פעילות הממונה על הפרטיות ברשות:

דו"ח הממונה על הפרטיות הוגש ביום 13.8.14 בהתאם לסעיף 33(ה) לחוק והועבר לגורמים הרלוונטיים המנויים בסעיף זה, לרבות רשם מאגרי המידע ברמו"ט. הדו"ח מפרט את עיקר פעילותו של הממונה על הפרטיות בשנה החולפת. בדו"ח פיקוח 2 צוין כי קיים ממשק מסודר בין הממונה על הפרטיות לצוות המקצועי ברמו"ט לשם מתן הבהרות, ובכלל זה התקיימה השתלמות על היבטים שונים של הגנת הפרטיות לעובדי הרשות על ידי רמו"ט. הממונה על הפרטיות עדכן כי הדו"ח השנתי מטעמו יוגש באוגוסט 2015, בהתאם לנדרש בחוק.

2.2.2. תכנית העבודה השנתית להיבטי הפרטיות וסקר סיכונים:

בדו"חות קודמים פורטו מסמכים אשר הוגשו לבקשת יחידת הממונה ובהם תכנית עבודה שנתית המתייחסת להיבטי פרטיות ומסמך איום ייחוס להיבטים אלה, מסמכים המתייחסים למימוש סעיף 25(3) לחוק (Privacy By Design), וכן נהלים נוספים העוסקים בתהליכי העבודה ברשות והנוגעים להיבטי פרטיות.

הממונה על הפרטיות העביר תכנית עבודה לשנת 2015. במסגרת תכנית זו עדכן הממונה על הפרטיות כי הרשות שכרה שירותי חברה חיצונית לביצוע סקר סיכונים אשר יבדוק את היבטי הפרטיות באופן מובחן, מעבר לסקר הסיכונים שכבר בוצע ברשות ב' על פי סעיף 10 לצו. כמו כן החברה תסייע בעיבוי המדיניות וכתובת הנהלים הקיימים.

תכנית העבודה של רשות ב' לשנת 2015 כוללת מהלכים נוספים לשיפור המעקב והניטור אחר פעולות הנוגעות למידע הביומטרי.

2.2.3. תפקידו של הממונה על הפרטיות ברשות ב' ותפקידים נוספים המוטלים עליו:

בעקבות ההערה שניתנה בדו"חות קודמים לבחינת היחס בין תפקידו של הממונה על הפרטיות לתפקידיו האחרים, נעשה טיפול על ידי הלשכה המשפטית של משרד הפנים ורשות ב' ליצירת הסדר מתאים. התייחסות לנושא זה הופיעה בדו"ח פיקוח 2.

2.2.4. הרשאות הגישה למערכות המחשוב של רשות ב' (הזדהות משולשת):

הגישה למערכות המחשוב כנדרש בתקנה 14(ד) נבדקה על ידי יחידת הממונה. מערך הגישה הודגם בעת ביקור ברשות ב' לקראת הוצאת דו"ח פיקוח 2 ונמצא כי היא תואמת לתקנה הנ"ל.

2.2.5. תקנות הממונה על הפרטיות:

הממונה על הפרטיות עדכן כי נוסח תקנות הנוגעות לביצוע תפקידו מצוי בעבודה משפטית. טיוטת התקנות הועברה ליחידת הממונה.

2.2.6. רישום המאגר הביומטרי ברשם מאגרי מידע על פי חוק הגנת הפרטיות תשמ"א 1981:

הממונה על הפרטיות עדכן כי המאגר הביומטרי נרשם כדין אצל רשם מאגרי המידע ברמו"ט. רמו"ט מסרה כי לאחר הליך היועצות ממושך, הוחלט על רישומו הנפרד של המאגר הביומטרי ממאגר המידע של רשות האוכלוסין. בירור סוגיה זו נדרש נוכח השתייכותה של רשות ב' והמאגר אותו היא מנהלת למשרד הפנים, שלו מאגרים רשומים לרבות מרשם האוכלוסין. מאגר המידע הביומטרי הלאומי נרשם בתהליך נפרד בתום ההליכים הנדרשים ובהתאם לנוהל המקובל ברמו"ט והוא כלול כיום בפנקס מאגרי המידע, הפתוח לעיון הציבור.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נספח ד' – תגובת הרשויות לטיוטת הדו"ח המסכם

תגובת רשות א' מוצגת להלן.

תגובת רשות ב' - ב-5.7.15 נמסר שאין להם הערות לטיוטת דו"ח הפיקוח המסכם.

תגובת רמון"ט - ב-5.7.15 נמסר שאין להם הערות לטיוטת דו"ח הפיקוח המסכם.

תגובת החטיבה - ב-6.7.15 נמסר שאין להם הערות לטיוטת דו"ח הפיקוח המסכם.

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219

י"ח תמוז תשע"ה
05 יולי 2015

לכבוד
מר רם ולצר, הממונה על היישומים הביומטריים
משרד ראש הממשלה

הנדון: התייחסות לטיטות דו"ח הפיקוח המסכם לתקופת המבחן

טיטות דו"ח הפיקוח המסכם לתקופת המבחן התקבל לידי רשות האוכלוסין בתאריך 30.06.2015, להלן התייחסות הרשות לממצאי טיטות דו"ח הפיקוח:

1. חלופת התשאול, סעיף 1.4.4 - לאחר קיום התייעצות במשרד המשפטים הוחלט ברשות האוכלוסין, עוד בשלהי שנת 2014, לתקן את סעיף 8 בצו לאור הצורך בשינוי שיטת בדיקת חלופת התשאול. גובש נוסח לתיקון הצו והוא הועבר למשרדי המשפטים והאוצר לצורך קיום חובת התייעצות כנדרש בחוק. ואולם, נוכח פיזור הכנסת והקדמת הבחירות לא ניתן היה לסיים את התהליך. אנו נדרשים לקבל אישור על קיום חובת התייעצות משרי המשפטים והאוצר ולאחר מכן יידרש אישור ועדת הכנסת המשותפת. הנושא מצוי בטיפול בלשכת השר.
התיקון המוצע כולל גם תיקון סעיף 10(ה) לצו (עניין המוזכר אף הוא בטיטות דו"ח הפיקוח).
2. החלפת סורקים, סעיף 1.6.2.2 - בעמדות הביומטריות במערך ביקורת גבולות לא הוחלפו סורקי טביעות האצבע, ולמעשה משתמשים בסורקים מולטי ספקטריים. חשוב לציין כי נמצא שביצועי האימות של דרכונים שהורכשו עם הסורק החדש (אופטי) מול טביעת אצבע הניטלת במעבר עם סורק מולטי ספקטרי, טובים יותר מדרכונים שהורכשו עם סורק מולטי ספקטרי (הישן) והם קרובים לביצועים המוצהרים על ידי היצרן. מבחינת ביקורת הגבולות אין צורך להרכיש מחדש ט.א שהורכשו עם סורקים מולטי ספקטריים, שכן המערכת עושה שימוש גם בביומטרית פנים לאימות העובר, כך שהביצועים המשולבים נותנים תוצאות משביעות רצון.
3. נספח ג', סעיף 2.1.5 - במסגרת סקר הסיכונים נעשתה הבחנה ברורה בין נושאי אבטחת מידע לנושא הפרטיות. כראיה לכך, בוצע תהליך שלם ומקיף (כרבע משעות הביקורת שהוקצו בסה"כ לסקר) על מנת לבחון את יכולת הפגיעה בפרטיות האזרחים על ידי עובד מרכז ההנפקה. במהלך הבדיקות, התבקשו אנשי החברה המבצעת את הסקר לנסות ולחדור לרשת מרכז ההנפקה במטרה לצפות או לשנות נתונים תחת הרשאות עובד בלבד (הרשאות נמוכות), כאשר מטרתם העיקרית היתה הגעה לנתונים על מנת לצפות בהם או לשנותם.

לאור האמור, במהלך הסקר נעשתה בדיקה מקיפה לנושא יכולות העובד הפשוט לפגוע בפרטיות הנתונים במרכז ההנפקה.

4. נספח ד', סעיף 4.8 - במהלך החודשים האחרונים, דיווחה רשות האוכלוסין מספר פעמים כי תהליך ביצוע שאילתות הושלם וכי הוא נמצא בבדיקות בין המאגר לבין הרשות. עד היום לא הועלתה שום דרישה מצד יחידת הממונה לקבלת מסמך המפרט את אופי הפתרון והתהליך. לאור בקשת היחידה כאמור מיום רביעי האחרון, נשלח מסמך מסכם ליחידת הממונה המפרט את הפתרון בצורה מעמיקה.

בברכה,



ברוך דדון

מנהל אגף פרויקטים

רשות האוכלוסין וההגירה

העתקים:

מנכ"ל רשות האוכלוסין וההגירה, מר אמנון בן עמי
מנהל אגף מערכות מידע, מר יוגב שמני
מנהלת האגף לתכנון מדיניות, גב' מרב אברהם
מנהל אבטחת מידע, מר עידו תלמי
לשכה משפטית, עו"ד עירית וייסבלום



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס (נספח ב' מסווג סודי)-

נספח ה' - הנתונים עליהם התבססה המלצת הוועדה המייעצת
בנוגע למאגר מבוסס על תמונת פנים בלבד

כתובת לקבלת דואר: קפלן 3, הקריה, ירושלים 91919

בית אמות משפט, שד' שאול המלך 8 קומה 5 תל אביב, טל' 03-7779222 פקס 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

תאריך: 5 יוני 2015

סימוכין: 0409-1

חלופת זיהוי פנים – אסמכתאות להמלצה1. רקע:

1.1 במסגרת תהליך גיבוש ההמלצות של הוועדה המייעצת המפקחת על התנהלות תקופת המבחן ובחינת תוצאותיה, בחנה יחידת הממונה על היישומים הביומטריים אסמכתאות ממקורות שונים בנושא חלופת זיהוי פנים.

1.2 ב-7.5.2015 הזמינה הוועדה המייעצת, את נציגי משטרת ישראל לדיון בו הוצגו המלצות הוועדה לתקופת המבחן לפני נציגי המשטרה. מספר ימים קודם, התקיים דיון עם סני"צ דוד אטיאס – ראש מעבדת ט"א במז"פ ועו"ד נירית להב קניזו, כהכנה לקראת דיון הוועדה המייעצת (עקב נסיעתו של סני"צ אטיאס לחו"ל ואי יכולתו להשתתף בדיון הוועדה המייעצת). לקראת הדיון הועברה למשטרת ישראל מצגת שבה הוצגו עיקרי הממצאים וטיוטת המלצות הוועדה.

1.3 בהמשך לדיון הוועדה המייעצת (7.5) ובהינתן התייחסות המשטרה בדיון, הוחלט לקיים פגישת עבודה מקצועית עם הגבי נטע לב-טוב – ראש מעבדת ראיות אלקטרוניות והאלבום המשטרתית, ובה לשמוע שוב את עמדות המשטרה ולהסביר ביתר פירוט את שיקולי יחידת הממונה והוועדה המייעצת, בעת המלצתם על חלופת הפנים. בפגישה זאת לא חולק חומר נוסף, אלא התקיים דיון על בסיס המצגת שהוזכרה לעיל ומצע לדיון שהוכן על ידי היחידה. בפגישה הוזכרו אסמכתאות שונות הקשורות לתהליך הבדיקה על ידי היחידה לרבות הפניה למסמכי ה-NIST, למסמכים של יצרנים ולמידע גלוי שקיים באינטרנט.

1.4 במהלך פגישה זאת, ביקשה משטרת ישראל לקבל תיעוד בכתב של האסמכתאות האמורות.

2. מטרה: מטרת מסמך זה הינה ריכוז האסמכתאות עליהן התבססה יחידת הממונה בהמלצה לגבי חלופת זיהוי הפנים, ואשר אליהם התייחסו בעת שהוצגו בדיונים שהתקיימו בנושא בין יחידת הממונה למשטרה.

3. שיטה:

3.1 סוגי המקורות והאסמכתאות בהן נעשה שימוש, נחלקים לשלושה:

3.1.1 מקור ראשון לבחינת ביצועי אלגוריתמים של זיהוי פנים, הוא דוחות של ארגון ה-NIST¹ בארה"ב, המתייחסים לבדיקה השוואתית של מוצרי זיהוי פנים מסחריים. זהו מקור בלתי תלוי עם שקיפות מלאה. יתרון נוסף הוא בכך שהדוחות מתייחסים לשנים שונות (החל מ-2002 ועד ל-2013): פירוט ר' בסעיף 4 להלן.

3.1.2 מקור שני באשר לאיכות הפתרונות הוא הצהרות יצרנים ודיווחים שונים שלהם לגבי איכות המוצרים. כמובן שמקור זה יש לקחת בחשבון בזהירות, מטעמים ברורים. לעיתים ישנה הפנייה של היצרנים עצמם לדוחות ה-NIST עם הדגשה על היתרונות שלהם לעומת המתחרים: פירוט ר' בסעיף 5 להלן.

3.1.3 מקור שלישי הוא דיווחים גלויים שונים באתרי אינטרנט, המדווחים על מחקרים, יישומים ודיונים ציבוריים. ככל שמדובר בדיווחים המגיעים מגוף רשמי, רמת המהימנות נחשבת גבוהה יותר, בעיקר כאשר ישנם מספר דיווחים צולבים לגבי אותו נושא. המידע המעניין בהקשר זה הוא בעיקר המידע שמגיע מצד הלקוח, כאשר במספר מקרים הדגש המושם הוא על ההישגים הפונקציונליים של המערכת, כלומר – כמה "מתחזים" הצליחה לסייע לגלות, ופחות על הביצועים הטכניים של המערכת.

¹ National Institute of Standards and Technology



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

בלמ"ס-

3.2 התייחסות למקורות השונים בהקשר להצגתם בוועדה המייעצת ובמשטרה:

3.2.1 חלק מהמקורות הוצגו בצורה מפורשת במהלך דיוני הוועדה המייעצת, כולל התייחסות אליהם במצגת שהוצגה בוועדה ושנשלחה למשטרת ישראל.

3.2.2 חלק מהמקורות הינם פרסומי יצרנים. הנושא של דיווחי יצרנים עלה בישיבה עם משטרת ישראל (בה נוכח גם יועץ הרשות לניהול המאגר הביומטרי). האסמכתאות המפורטות כאן הינן מהוות "מראה מקום" מדויק לדוגמאות שהוצגו ונדונו בעל פה. מדובר על יצרנים קוגניטק וקוגינט ו- NEC שהוזכר בדוחות ה- NIST כיצור בעל הביצועים הטובים ביותר.

3.2.3 המקורות האחרים מתייחסים ליישומים במדינות שונות. חלק מהמקורות קיימים במסגרת דיווחי הרשויות – בסדרת הדוחות לגבי הצדקת הצורך במאגר, ובחלקם דוח המסכם של הרשות לניהול המאגר הביומטרי. אסמכתאות אלו נבחנו לעומקם מעבר לאיזכורם כהפנייה (reference).

3.2.4 מקורות נוספים אותרו בחיפוש עצמאי באינטרנט, להשלמת התמונה.

3.3 על מנת להקל, מרוכזים בטבלה הבאה האסמכתאות השונות וסיווגן בהתאם לסעיף 3.2 דלעיל:

ספ'	האסמכתא	סעיף במסמך	מקור	אופן הצגה למשטרה
1	דוח NIST 8009	4.2	גלוי, אתר ה- NIST	במצגת, בדיון: מקור זה היה מוכר למשטרה.
2	דוח NIST 7709	4.3	גלוי, אתר ה- NIST	בדיון. מקור זה היה מוכר למשטרה.
3	ביצועי היצרן קוגניטק	5.2	גלוי	נתוני הביצוע צוינו בדוח של הרשות לניהול המאגר הביומטרי. הוזכר בדיון.
4	ביצועי היצרן קוגינט	5.3	גלוי	בדיון.
5	ביצועי היצרן NEC	5.4	גלוי	מוזכר בדוחות NIST, בדיון.
6	קנדה	6.2	גלוי	במצגת, בדיון.
7	ניו-זילנד	6.3	גלוי	מוזכר במסמכי הרשות לניהול המאגר הביומטרי; במצגת; בדיון.
8	יישומים במדינות שונות בארה"ב	6.4	גלוי	מוזכר במסמכי הרשות לניהול המאגר הביומטרי; במצגת; בדיון.
9	יישומים משטרתיים	6.5	גלוי	הוזכר בדיון שישנם יישומים כאלו.



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

4. דוחות NIST:

4.1 הדו"חות הרלבנטיים ביותר הם:

4.1.1 דו"ח FRVT שנערך ב- 2013 ופורסם ב- 2014 תחת השם NIST Interagency Report 8009
http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf

4.1.2 דו"ח NIST Report on the Evaluation of 2D Still-Image Face Recognition Algorithms
 : Interagency Report 7709

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968

4.1.3 להלן פירוט לגבי כל דו"ח בסעיפים 4.2, 4.3 להלן.

4.2 דו"ח 8009 מ- 2014:

4.2.1 דו"ח זה כולל קביעות רבות המסבירות את השיפורים שחלו בטכנולוגיה זאת בשנים האחרונות ובפרט לעומת הדו"ח הקודם של שנת 2010.

4.2.2 להלן תקציר המנהלים של הדו"ח. נקודות משמעותיות מובלטות בהדגשה.

Technical Summary

Absolute accuracy: When **mugshot images** from 1.6 million individuals are enrolled by the most accurate algorithm, 4.1% of subsequent mated searches fail to yield the correct mate in rank one position. Practically this result assumes that a human reviewer will be employed to adjudicate the candidate identities. If, on the other hand, a threshold is elevated to limit false positive outcomes to only 1 in 500 searches (0.2%), the failure to find the mate rises to 7.5%. Using **poorly constrained webcam images**, which exhibit serious departures from most quality-related clauses of published image standards, identification miss rates are typically between two and five times higher such that the correct mate is not found at rank one in 20-60% of searches. Exceptionally, however, the most accurate algorithm fails in only 11.3% of searches. This latter result is notable in that it indicates that face recognition can work on non-ideal images. Thus, while the webcam images were collected

from nominally cooperative subjects, the use of inferior equipment and procedures means, for example, that images from non-cooperative bank ATM machine and surveillance camera deployments will be recognizable in a useful number of cases.

Accuracy across commercial providers: Recognition accuracy is very strongly dependent on the algorithm and, more specifically, on the developer of the algorithm. Recognition error rates in a particular scenario range from a few percent up to beyond fifty percent. Among the most accurate developers, the rank one miss rates for recognition in a population size of 1.6 million are 4.1% (NEC), 9.1% (Morpho), 10.7% (Toshiba), 13.6% (Cognitec), 17.2% (3M) and 20.5% (Neurotechnology). For webcam images, this sequence is 11.3% (NEC), 23.7% (Toshiba), 29.8% (Morpho), 36.4% (3M), 57.6% (Cognitec) and 66.9% (Neurotechnology). While results for up to six algorithms from each developer are reported here, the intra-provider accuracy variations are usually smaller than the inter-provider variations. That said, some developers submitted different, less accurate but computationally lightweight algorithms.

Accuracy under increasing population size: As more identities are enrolled into a biometric system, the possibility of a false positive increases due to lookalike faces that yield extreme values in the tail of the non-mate score distribution. However these scores are lower than most mate scores such that when an identification is configured with a threshold of zero, and where human adjudication is always necessary, rank-one identification miss rates scale very favorably with population size, N , growing approximately as a power law, aN^b . Depending on the algorithm, the exponent b for mugshot searches is low, on the range [0:08; 0:16] meaning that a large, 10-fold, increase in N , yields only a 1.2 to 1.4 fold increase in the rate at which mated searches do not yield the correct mate. Thus the rank one mugshot miss rates, for search into a database of just 160,000, are only modestly improved over those at 1.6 million: 4.1% to 3.4% (NEC), 9.1% to 7.6% (Morpho), 10.7% to 7.9% (Toshiba), 13.6% to 10.9% (Cognitec), 17.2% to 13.3% (3M) and 20.5% to 16.9%



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

בלמ"ס-

(Neurotechnology). While extrapolation to larger populations is technically problematic, face identification systems will be useful, if imperfect, in nation-state population sizes.

Utility of adjudicating long candidate lists: In the regime where a system is configured with a threshold of zero, and where human adjudication is always necessary, the reviewer will find mates on candidate lists at ranks far from one. The accuracy benefits of traversing such lists are usually substantial: For example, in a population of 1.6 million, the rank one and rank fifty miss rates are 4.1% to 2.6% (NEC), 9.1% to 7.1% (Morpho), 10.7% to 5.7% (Toshiba), 13.6% to 8.4% (Cognitec), 17.2% to 9.8% (3M) and 20.5% to 13.6% (Neurotechnology). These are diminishing returns, however, with miss rates for some algorithms growing as power-law, aR^c , in the number of candidates a reviewer is willing to consider, R . The exponent c for mugshot searches is typically on the range $[0.2; 0.1]$ indicating that rank 1 miss rates are reduced by from 20% to 40% if 10 candidates are available for inspection, but only by 30% to 50% if 50 are considered.

Human adjudication workload: Human reviewers will typically only need to search the first few (highest scoring) candidates returned in a search. The expected number of comparisons constitutes a workload measure which can be used to both compare algorithms and to inform operational labor requirements. If a score threshold is applied to reduce the length of candidate lists, substantial reviewer workload reductions can be realized but at the expense of increased miss rates. In the best case, application of a threshold to candidates from a Morpho algorithm reduced workload by 60% with only a factor of 1.05 more misses than without a threshold.

Accuracy by age group: Identification accuracy is strongly dependent on subject age. For all algorithms, older individuals are both easier to recognize as themselves, and easy to tell apart from each other. The opposite is true in children: both false negative and false positive rates are much higher, with infants being very hard to identify. Moreover, the trends are progressive throughout adulthood, with young adults being identified with worse accuracy than older. These results are derived over images taken, on average, 2-3 years apart so the effects of ageing (craniofacial shape change) are influential only on the results for younger individuals.

Accuracy gains 2010-2013: For the four developers who submitted algorithms to NIST in 2010 and 2013, accuracy has improved in all cases. Rank one miss rates have reduced by about 10% for Cognitec, Neurotechnology, and Morpho, and by about 28% for NEC (from 8.9% to 6.4%). More substantial reductions have been realized when a threshold is applied to permit false positive outcomes in only 1 in 500 non-mate searches: There Morpho realizes a 21% reduction in misses (from 24.8% to 19.5%), while for NEC, the figure is 60% (26.9% to 10.8%). Finally the accuracy gains when reviewers examine up to 50 candidates are more modest, ranging from 3% (Cognitec) to 12% (Neurotechnology).

Sketch recognition: By searching a non-operational set of sketch images against photographs seeded into a population of 640,000 non-mated mugshots, the most accurate algorithms produce the mated photograph only infrequently: The mate is not among the top 50 candidates at the following rates: 73.3% (3M/Cogent), 73.8% (NEC), 78.5% (Toshiba), 80.3% (Morpho), and 81.5% (Neurotechnology). While these error rates are very high, they are nevertheless valuable in developing investigative leads in cases which are otherwise cold. An important caveat is that sketch-identification was never declared to be part of FRVT and better algorithms may be available from the providers. That said, face recognition algorithms are being used to recognize sketches operationally. Further accuracy will clearly be dependent on eye-witness recall, artist interpretation if any, and software interfaces.

Conclusions: As with other biometrics, accuracy of facial recognition implementations varies greatly across the industry. Absent other performance or economic parameters, users should prefer the most accurate algorithm. Note, however, that the results of this section are entirely rank-based befitting use of face recognition in the investigational mode in which a reviewer is willing to traverse candidate lists looking for mates. Subsequent investigations in this report consider threshold-based metrics appropriate for identification mode applications. Note that the absolute values of identification accuracy will always depend on the dataset used, specifically to the properties of the images in use. In particular, the main dataset used here includes



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

some images that are not perfectly frontal, such that conformance to the appearance-related requirements of the ISO/IEC 19794-5 "gold" standard is imperfect.

Improving face recognition: On the basis of the results in this report, we identify the following drivers of overall recognition accuracy, and quantify their relative influence relative on false negative miss rates.

Quality: Improvement of image quality is the largest contributing factor to recognition accuracy. Results in this report note a fourfold reduction in miss rates using mugshots vs. webcam images. Further improvements in accuracy can be obtained by enhancing conformance to the ISO/IEC 19794-5 "gold" standard [26], particularly using two complementary approaches: by design via improved optical and photographic aspects, and by careful application of compression algorithms; and by detection of non-conformant (for example, blurred or non-frontal) images at the time they are collected. A new program has been established to evaluate algorithms capable of detecting defective images [9, 10]. The best practice should be to collect and retain forensic quality photographs (i.e. subject acquisition profile 50/51 instances of the ANSI/NIST Type 10 standard [27]), from which ISO/IEC 19794-5 images should be prepared for automated recognition.

Human adjudication of candidate lists: Recognizing that a human is often involved in examining candidates produced in an automated one-to-many search, it is imperative that the enrolled reference "exemplar" image be of high quality. Given ready availability of high resolution digital cameras, the ANSI/NIST standard advocates collection of forensic quality images for which the interocular distance is around 800 pixels. Such images are not used directly for automated face recognition, so the default guidance is to collect and retain the forensic image, and to prepare from it the ISO standard image (120 pixels interocular distance) for automated face recognition. Accuracy can be improved by supplementing automated facial identification with human adjudication of the candidate photographs. Particularly by traversing long candidate lists (for example, up to length 50) miss rates can readily be reduced by a factor of two (i.e. 50%) An important caveat here is that the accuracy with which human reviewers can reliably adjudicate the most-similar faces returned in a large-population one-to-many search remains poorly quantified.

Algorithm selection: Algorithm performance varies substantially - even among the leading providers a factor of two reduction in identification miss rates can be realized by replacing one algorithm with a better one. Such a step should be undertaken only while paying due attention to other performance related factors, such as computational expense and impostor distribution stability.

דו"ח 7709 מ-2010 : 4.3

4.3.1 דו"ח זה הינו דוח חשוב בסיסי שכן לראשונה נבחנו בו אלגוריתמים של זיהוי (אחד לרבים) כפי שהם, ולא בהנחה של ביצוע $N \cdot 1$. כמו כן הדוח כולל השוואות לביצועים של שנים קודמות, כדי לקבל פרספקטיבה לגבי ההתקדמות בשנים שעברו.

4.3.2 להלן תקציר המנהלים של מהדו"ח. נקודות משמעותיות מובלטות בהדגשה.

EXECUTIVE SUMMARY

Background

— Facial recognition algorithms from seven commercial providers, and three universities, were tested on one laboratory dataset and two operational face recognition datasets, one comprised of visa images, the other law enforcement mugshots. The population represented in these sets approaches 4 million, such that this report documents the largest public evaluation of face recognition technology to date. The project attracted participation from a majority of the known providers of FR technology including the largest commercial suppliers.

— Accuracy was measured for three applications: One-to-one verification (e.g. of e-passport holders); one-to-one verification against a claimed identity in an enrolled database (e.g. for driver's license re-issuance); and one-to-many search (e.g. for criminal identification or driver's license duplicate detection).



The Biometric Applications Commissioner

-בלמ"ס-

— Face images have been collected in law enforcement for more than a century, but their value for automated identification remains secondary to fingerprints. In a criminal investigation setting, face recognition has been used both in an automated mode and for forensic investigation. However, the limits of the technology have not previously been quantified publicly, and, in any case, are subject to improvement over time, and to the properties of the images in use.

— Core algorithmic capability is the major contributor to application-level recognition outcomes. A second critical factor is the quality of the input images; this is influenced by design of, and adherence to, image capture protocols (as codified by face recognition standards) and also by the behavior of the person being photographed (e.g. whether they face the camera). Some data collection protocols can embed a human adjudication of quality (e.g. of a visa image by a consular official) while others cannot maintain such tight quality controls (e.g. because of non-cooperative subjects in police booking processes).

— This is the first time NIST has reported accuracy of face identification algorithms. Prior tests have assumed an equivalence of a 1:N search as N 1:1 comparisons. This new protocol formally supports use of fast search algorithms such as indexing, partitioning and binning. The benefits are more accurate predictions of scalability to national-size populations.

— The project used archival imagery to assess core algorithmic capability of algorithms. It did not do an instrumented collection of images as might be used in a scenario or operational test. It therefore did not measure human-camera transactional performance parameters such as duration of use and outcome. These would be of vital interest in, for example, e-Passport gate applications.

Core Accuracy

— As with other biometrics, recognition accuracy depends strongly on the provider of the core technology. Broadly, there is an order of magnitude between the best and worst identification error rates.

— Biometric identification algorithms return candidate lists. These enumerate hypothesized identities for a search sample. Face identification algorithms can be set up to be used in two distinct modes. The first, *investigational* mode, assumes the existence of a corps of human face examiners retained to examine perhaps dozens of images on candidate lists. In the second, *identification* mode, the algorithm is set up with a high threshold to give very short candidate lists and a small chance that a non-matching candidate is returned. The most accurate investigational algorithms are not the most accurate identification algorithms.

— Using the most accurate face recognition algorithm, the chance of identifying the unknown subject (at rank 1) in a database of 1.6 million criminal records is about 92%. For other population sizes, this accuracy rate decreases linearly with the logarithm of the population size. In all cases a secondary (human) adjudication process will be necessary to verify that the top-rank hit is indeed that hypothesized by the system.

— When the most accurate algorithm is used in an investigational mode to provide trained examiners with the top fifty ranked candidates 97% of searches will yield the correct identity in a fixed population of 1.6 million subjects. In cases where the top 200 candidates are searched, the correct match is present 97.5% of the time. The hit rate increases roughly linearly with the log of the number of candidates inspected.

— In criminal law enforcement applications, where recidivism rates are high and a pool of examiners is available to traverse lengthy candidate lists, facial recognition algorithms offer high success rates. The more accurate algorithms reduce the workload on the examiner by placing mates at low (i.e. good) rank. We define an overall performance metric as the expected number of candidates an examiner will need to compare before the mate is found. If the most accurate algorithm is used for identification in the population of 1.6M, an examiner willing to review 50 candidates will only need to look at 3 on average before the mate is found.

— A facial recognition algorithm can also be used to do “lights-out” face identification. This requires application of a high decision threshold that implements a selectivity policy. Here a threshold is adopted that gives, on the average, a particular number of false candidates per search. For the most accurate face recognition algorithm tested here, if one in two searches produces a false candidate on average, the hit rate



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

will be 89%. If workload demands on human adjudicators require that only one in ten searches produce a false candidate, the hit rate reduces to 85% and a different algorithm is best in this regime. These numbers apply to a population of 1.6M. The threshold will need to be estimated over a calibration process. This threshold will need to be increased as the enrolled population increases.

— Facial recognition algorithms are more accurate on the visa images than the mug shot images. The visa images were collected c. 1996-2001. The imaging processes used for their collection have improved since that time. The mug shot images are contemporary, and operationally representative of current law-enforcement collection practices. On these images, the face recognition accuracy results reported here will be closely predictive of those that would be encountered in any near term deployment.

— The visa images are collected with careful cooperation of the subject, active compliance by the photographer to the image collection specification, and a yes/no review by an official. The visa images are subject to losses associated with JPEG compression. The mugshot images, while less compressed and of generally higher resolution, exhibit considerable pose, illumination and expression variation. The most accurate algorithm demonstrates better tolerance of non-frontal pose than others.

— On the one database used in 2002, 2006 and 2010, the best verification accuracy measurement has declined by an order of magnitude in each four year period. On the visa images, false non-match rates (at a fixed false match rate of 0.001) have reduced from 0.2 in 2002, to 0.026 in 2006, and to 0.003 now. This result is achieved on a dataset that has various deviations from formal standards and best practices.

Exploitation of all historical encounters

— The test was executed using an Application Programming Interface (API) that supported identification of an image against all prior images of a subject, not just the most recent. This allowed the face recognition algorithm developers to exploit the historical record. It also assigned responsibility for fusion to the algorithm developers, who could implement early-stage template-level fusion or the simpler late stage score-level fusion.

— All recognition algorithms derive accuracy improvements when all past images are enrolled as a single template. The benefits are uniform across algorithms. The template size for a person enrolled with K images is, for all algorithms tested, closely K times the template size produced from a single image. These two facts suggest that common and simple techniques are sufficient to realize the available gain.

Speed and template size

— For the first time, this NIST evaluation measures and reports the speed of face recognition algorithms. The main result is atypical in biometrics: The most accurate algorithms are among the fastest. This departs from observations in fingerprint and iris trials that showed an industry-wide tradeoff between accuracy and computational expense.

— For search algorithms from the two most accurate providers, the time required to execute a one-to-many search against an enrolled population of 1.6 million people is 0.4 and 1.2 seconds respectively. This is the duration of the core search computation as measured on contemporary high-end yet standard hardware consisting of 16 computational cores, 192GB of main memory, and a 64 bit address space. It assumes that a search template has been prepared and transmitted to the matching engine.

— In most cases the time required to execute a search does not scale linearly with the size of the enrolled population. While the most accurate algorithm does scale linearly, the second most accurate algorithm scales such that a ten-fold increase in database size produces only a 1.3-fold increase in search duration. This behavior has been confirmed on sizes up to 1.6 million.

Several participants elected to provide several implementations for evaluation. In so doing the provider demonstrated an ability to trade accuracy for speed, and to use large or small template sizes. This suggests a valuable ability to parameterize their algorithms to meet computational and accuracy requirements.



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

— The variance in search times is small. This arises because all search templates from a particular recognition algorithm have the same size. Across the algorithms tested here, template sizes range from about 5 to 75 kilobytes. By comparison, 90% of the law enforcement JPEG images used here are in the range 4 to 380 kilobytes, with median, 36 kilobytes.

Accuracy dependence on biographic data

— For the law enforcement images, it is empirically observed that men are more easily recognized than women, that heavier individuals are more easily recognized than lighter subjects, and that Asian subjects are more easily recognized than White. Younger persons are more difficult to recognize than their elders for some recognition algorithms, but the opposite is true for others.

— These results state marginal observations for the particular dataset. They do not explain the cause of the observation because there are confounding aspects to the data. So while men are more readily recognized than women, this may arise because women are generally shorter than men, and the height of a subject may induce non-optimal imaging angle if the camera height is not adjusted.

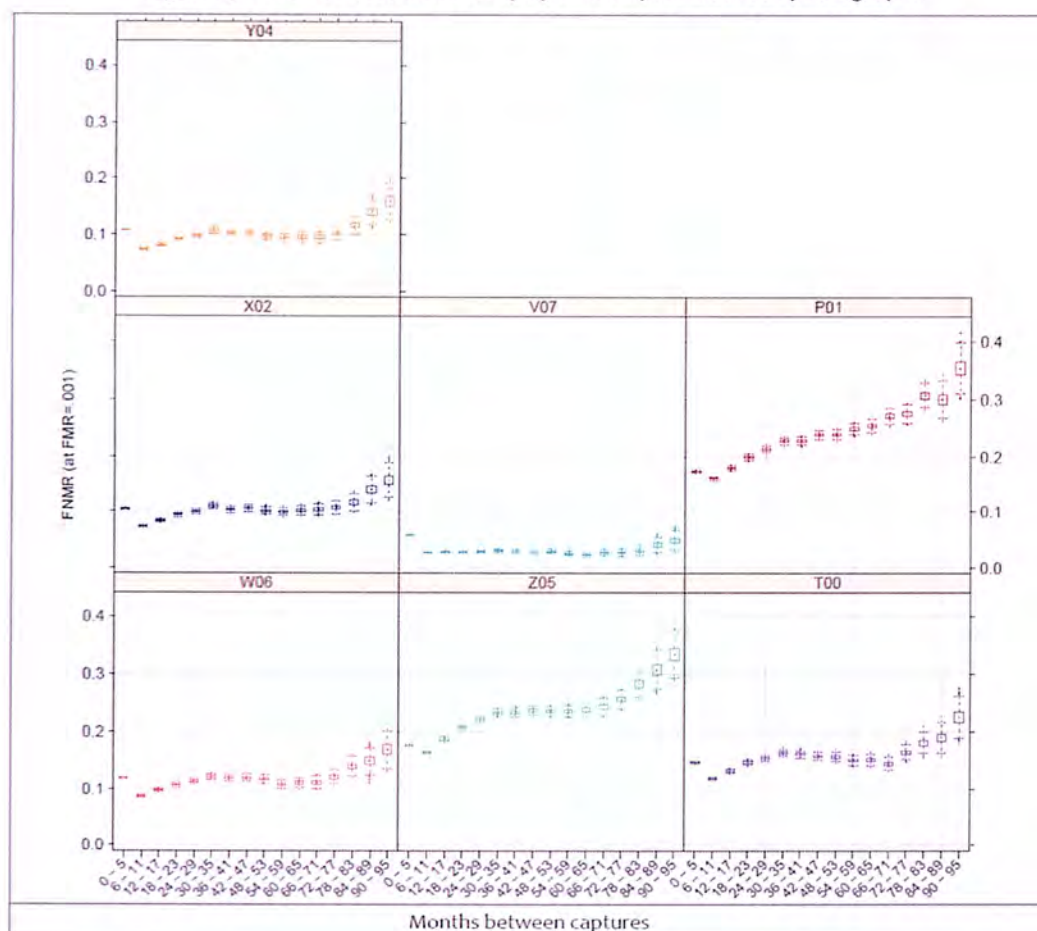
4.3.3 להלן קטע מהדו"ח העוסק בהשפעות משך הזמן בין הצילומים על דיוק התוצאות:

X02 – קוגניטק

NEC = V07

Cogent – לא מופיע

Figure 25 – LEO Verification accuracy by time elapsed between photographs





הממונה על היישומים הביומטריים
The Biometric Applications Commissioner

-בלמ"ס-

5. הצהרות יצרנים

5.1 כללי:

5.1.1 הצהרות יצרנים הינן כלי נוסף להערכת רמת הדיוק של המערכות השונות המוצעות על ידיהם. ההנחה היא שכל יצרן ירצה להבליט מבחינה שיווקית את יתרונות האלגוריתמים שלו, אבל יחד עם זאת יהיה מחוייב לדווח דיווחי אמת.

5.1.2 כפי שנאמר בדוחות ה-NIST שצוטטו לעיל, איכות האלגוריתם הינה המרכיב החשוב ביותר, לצד איכות התמונות, ביכולת להגיע לרמת זיהוי גבוהה.

5.1.3 היצרנים הנחשבים כיום כמובילים בתחום זה הם Toshiba, 3M/Cogent, Sagem/Morpho, NEC ו-Cognitec. הנתונים דלעיל הם של החברות עצמן או פרסומים המציגים את המוצרים לפי הצהרות היצרנים.

5.2 חברת קוגניטק (Cognitec)

5.2.1 להלן מספר פרסומים לגבי מנוע B6T8:

5.2.1.1 הודעה על שחרור המוצר בחודש דצמבר 2011:

<http://www.planetbiometrics.com/article-details/i/959/>

5.2.1.2 גרף ביצועי האלגוריתם:

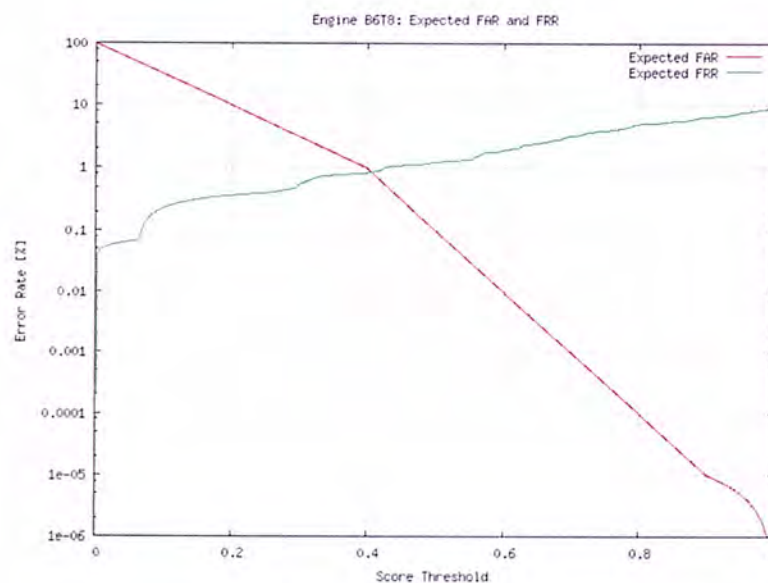


Figure 1.3: FAR / FRR rates mapping of B6T8

5.2.2 בפרסום הבא ניתן לראות את התפתחות המוצרים לאורך השנים, עם הערות של היצרן עצמו לגבי המוצרים –

<http://www.cognitec.com/independent-vendor-tests.html>

5.2.3 בין היתר ניתן לראות התייחסות לביצועי המערכת בשנת 2010 בהתאם לבדיקות ה-MBE –NIST:

MBE 2010: In the latest NIST test, conducted in 2010, seven companies and three research institutes participated in the MBE-STILL evaluation, comparing the performance of face recognition algorithms on still images. Cognitec again delivered excellent performance in all the tests. In the open-set identification test, the

כתובת לקבלת דואר, קפלן 3, הקריה, ירושלים 91919
שד' שאול המלך 8, תל אביב, טל: 03-7779222, פקס: 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

most relevant for challenging identification applications, Cognitec's algorithm had the best performance at the lowest false alarm levels, which corresponds to the operational setting with a multi-million gallery and limited resources for visual inspection.

5.2.4 לגבי הבדיקות של ה-FRVT של ה-NIST משנת 2013, העדיפו להדגיש את היתרון באלגוריתם זיהוי הגיל, נושא אליו התייחסנו כאפשרות לשיפור תהליך הזרימה והתייעלות, כדלקמן:

FRVT 2013: Test results on the performance of automated age estimation algorithms confirmed Cognitec Systems' leading position in the face recognition market. The test compared nine algorithms submitted by six participants, five companies and one university, and applied them to seven million images. Results show that Cognitec's algorithm performs with the highest accuracy for all age groups. Most notably, the algorithm shows superior performance "in the youth and senior age groups, leading the next most accurate algorithm in 5-year accuracy by 30% and 16%, respectively," according to the report.

5.2.5 לגבי האלגוריתם החדש של קוגניטק, B9, נאמר שם כי יש בו שיפורים נוספים משמעותיים לעומת האלגוריתם שנבדק ב-FRVT של 2013, כדלקמן:

The last independent testing of leading face recognition engines was conducted in 2013, with results published by NIST in 2014. Our current matching algorithm B9 shows significant performance improvements compared to the algorithm evaluated during 2013 NIST tests.

5.2.6 בהמשך מובאים הנתונים עצמם של אלגוריתם זה (B9), לעומת הדור הקודם (B8):

B9T8 Algorithm Performance

The following three diagrams show the performance of the current B9T8 engine and, for reference, the previous engine B8T8 in the closed-set identification, the open-set identification and the verification scenario.

All measurements were done using the same set of low-quality facial images. Most images of that set show a face that is either blurry, in low resolution, badly illuminated (with over- or underexposure, or hot spots), in a distinctly non-frontal pose, or exhibit a combination of those conditions. For the performance measurements, the set was divided into a gallery containing 518 images of 518 subjects (i.e. one image per subject) and a probe gallery consisting of 699 images of 254 subjects (each of which also occurs in the gallery).

The performance measures applied in the diagrams are defined in the ISO/IEC 19795-1 standard: "Information technology – Biometric performance testing and reporting – Part 1: Principles and framework", 2006.

Disclaimer Face recognition technology, like any biometric application, cannot provide 100% recognition accuracy.



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-



Diagram 1: Closed-set identification performance on the set of low-quality face images

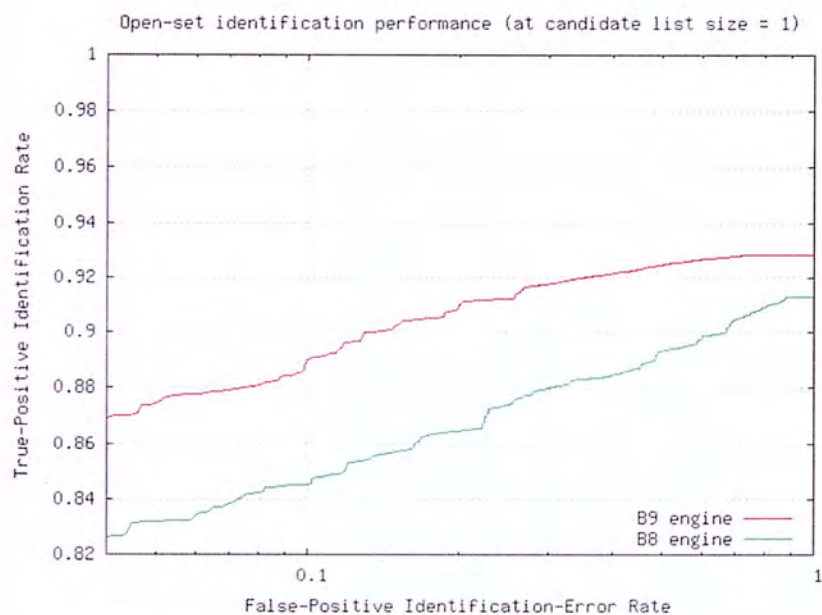


Diagram 2: The open-set identification performance curve reflects application scenarios for passport/visa or driver's license issuance and for video surveillance.



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

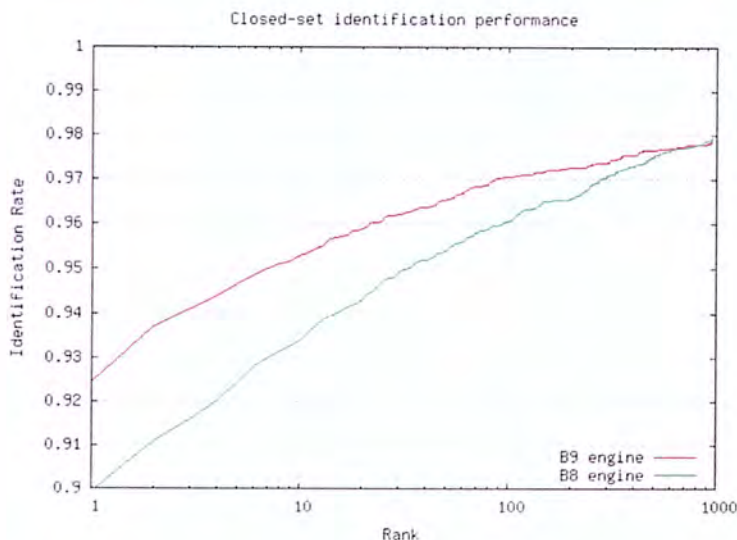


Diagram 4: Closed-set identification performance in the pose variation test

The rank 1 identification rate has increased from 90% to 92.5%.

Diagrams 6 and 7 show the performance on faces in low resolution. For the measurements, a gallery of 4108 faces of 4108 different subjects was matched with a probe set of 7677 different faces of 4114 different subjects (the same subjects as in the gallery, except for a few), resulting in 7654 genuine scores and more than 31 million imposter scores. The images are in passport style, mildly affected by JPEG compression artifacts, and mostly of Caucasian and African-American adults. The average inter-eye distance is 62 pixels.

All probe images were scaled down to achieve an inter-eye distance of 20 pixels, while the gallery images were left at their original size. This corresponds, for example, to a video surveillance situation where the gallery consists of good quality photographs and the probes are extracted from video footage taken with a typical video camera.

Further improvements over the previous engine B8

In the development of the engine B9 we focused on improving the recognition performance on difficult image material, in particular images with faces in low resolution or in non-frontal poses, which are typical for video surveillance applications. The four diagrams on the next two pages show the performance increase over B8 on such images.

In diagrams 4 and 5, the performances of B8 and B9 are compared under head pose variation, using a set of 994 frontal pose images in the public Color FERET database as the gallery. The probe set consists of all non-frontal pose images from the Color FERET database in which both eyes are visible. Head poses up to half-profile are included in the probe set. For more information on the Color FERET database, see the articles listed under References.



הממונה על היישומים הביומטריים
The Biometric Applications Commissioner

-בלמ"ס-

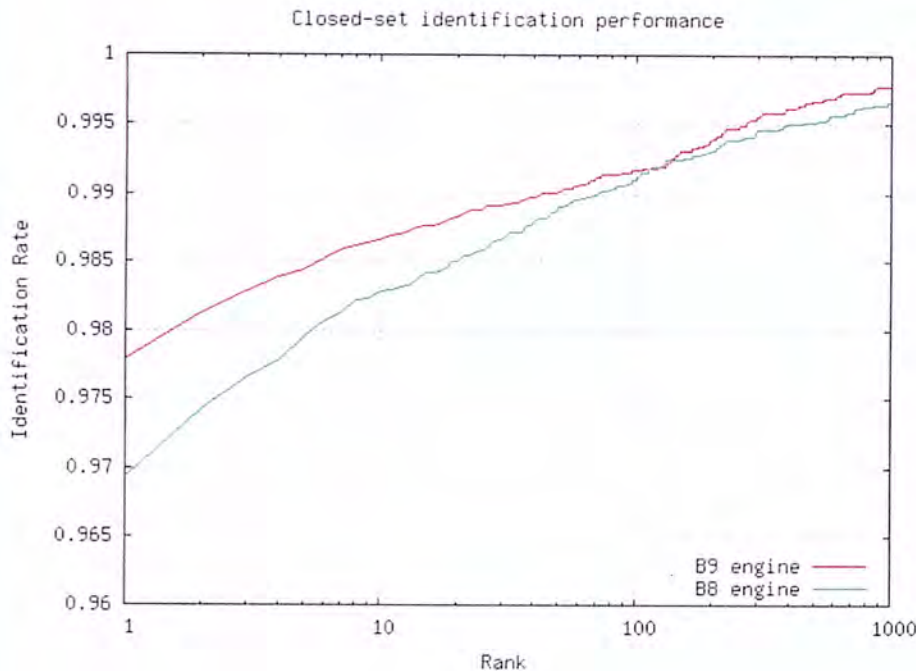


Diagram 6: Closed set-identification performance in the low resolution test

5.2.7 התייחסות לנושא תאומים זהים נמצאת בתיעוד המערכת FaceVACS ונותנת הערכה על הכמות שלהם באוכלוסייה:

FaceVACS-SDK C++ Reference Manual Version 8.8.0

1.7.4 FAR, FRR and Score

The result of a comparison between 2 FIR's is a score value in the range [0,1], higher values representing more similar feature sets. Due to inevitable differences between the samples, for example caused by varying facial expressions, poses or lighting conditions, comparing different FIR's of the same person will not yield maximum score values in any case. On the other hand, FIR's created from different persons might yield rather high score values, when they indeed are similar (e.g. there are 0.4 % monozygotic twins in the population). Hence, the result of face recognition can only be expressed in terms of probability.

5.3 חברת Cogent:

5.3.1 להלן פרסום של החברה לגבי המוצר שלה לזיהוי פנים:

<http://multimedia.3m.com/mws/media/833810O/facial-recognition-biometric-technology.pdf>

5.3.2 בפרסום זה כתוב בין היתר:

In December, 2008, just four years after it was released, the 3M Cogent Facial Recognition System squared off against the nine other industry-leading products in the National Institute of Standards and Technology Still Face Challenge Problem at the Multiple Biometric Grand Challenge (MBGC). 3M Cogent facial recognition software led in measured accuracy against all other vendors for both controlled and uncontrolled facial image comparisons. **Even in adverse lighting, image, and pose conditions, the 3M Cogent algorithms consistently scored in the top tier for high accuracy (90+%) at a low false accept rate (.001%).**

5.3.3 במסגרת השימושים מצוין כך:

כתובת לקבלת דואר, קפלן 3, הקריה, ירושלים 91919
שד' שאול המלך 8, תל אביב, טל: 03-7779222, פקס: 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

ID document issuance— For driver's licenses and other forms of government and commercial identification, 3M Cogent provides immediate face image capture, normalization, and 1:1 and 1:N identification.

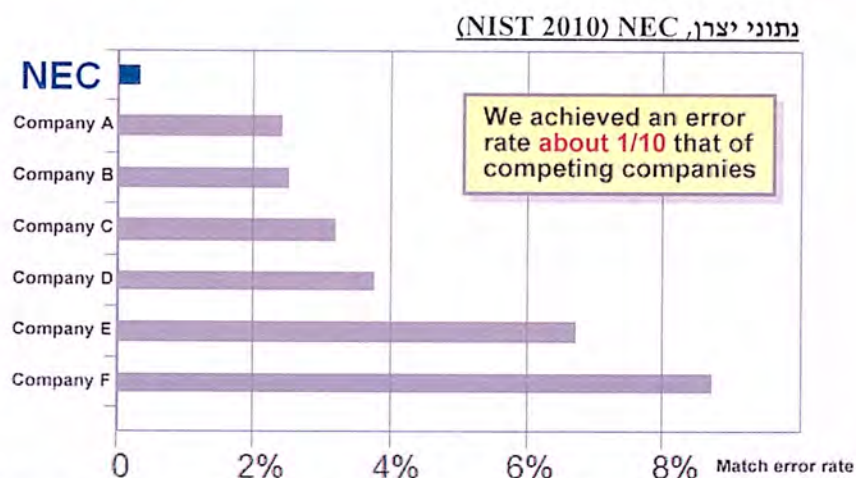
5.4 חברת NEC

5.4.1 חברה יפנית המצטיינת בביצועים שלה במסגרת מבחני ה- NIST כפי שניתן היה לראות בדוחות עצמם.

5.4.2 ניתן ללמוד על ביצועי החברה מתוך ראיון שהתקיים עם מהנדס המערכת

http://www.nec.com/en/global/innovators/h_imaoka/01.html

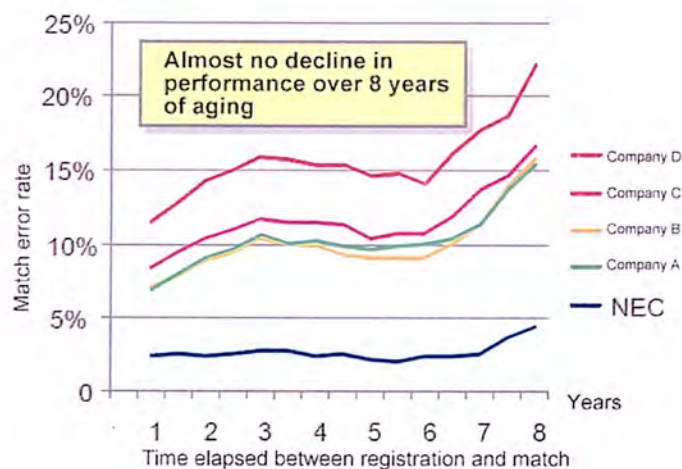
5.4.3 להלן חלק מהנתונים שהוצגו שם בנושא ביצועים :



NIST benchmark test results matching error rate comparison (False rejection rate when the false acceptance rate is 0.1%)

5.4.4 להלן נתונים שהוצגו בהקשר לירידת ביצועים עקב הפרשי גילאים בנטילת התמונות :

NIST benchmark test results Aging comparison (Changes in error rate over 1 to 8 years)





הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

6. יישומים בעולם:

6.1 כללי:

6.1.1 קיימים דיווחים רבים מהעולם על יישום מערכות זיהוי פנים. במסגרת זאת נתמקד בעיקר ביישומים עבור תהליכי מניעת זיופים והונאות להנפקת תיעוד מזהה. עיקר הדיווחים הם ממדינות שבהן אין ככלל איסוף של טביעות אצבע מאזרחים עבור הנפקת תיעוד. התיעוד הרלבנטי מתייחס להנפקת דרכונים ולהנפקת רישיונות נהיגה.

6.1.2 בין המדינות הבולטות בתחום זה הן קנדה, אוסטרליה וני-זילנד. בנוסף, בריטניה פרסמה מכרז בינלאומי גדול עבור מערכת הנפקת הדרכונים שלה שמבוססת על זיהוי פנים בלבד. יישומים בולטים נוספים הם בארה"ב ב- 37 מדינות (states) אשר משתמשות במערכות זיהוי פנים בלבד לפני הנפקת רישיונות נהיגה שמהווים דה-פקטו מסמך זיהוי במדינות אלו כולל לבני נוער.

6.2 קנדה:

6.2.1 המשרד להנפקת דרכונים בקנדה מפרסם באופן שנתי דוחות באשר למדיניותו ופעילותו. בין היתר ניתן דגש בשנים האחרונות על השימוש במערכת זיהוי פנים, כרכיב חיוני ומוצלח.

6.2.2 המערכת יושמה בשנים 2010 – 2011. להלן ציטוט מתוך הדוח השנתי ל- 2010 – 2011
<http://www.cic.gc.ca/english/resources/publications/passport-ar/2010/index.asp>

In 2010–2011, we put in place the foundation we need for future transformation. Key among these accomplishments was making facial recognition (photo-matching) fully operational. We are the only federal government organization with this capability. It vastly improves the accuracy and speed of identity verification and our ability to detect fraud.

6.2.3 במסגרת ההישגים לשנים אלו הם מציניים:

Implemented a new facial recognition (FR) (photo-matching) technology. All passport applications are now being processed through the FR system strengthening the integrity of the entitlement process.

6.2.4 נתוני תוצאת יישום המערכת מוצגים להלן:

Security and Fraud Detection

In 2010–2011, our facial recognition (photo matching) system which compares the photos provided with passport applications to the photos we have on file, resulted in the recall of 49 passports and 46 referrals to Passport Canada's identity fraud desk for further investigation.

Investigations into concerns related to identity, suspected fraudulent activity or misuse of a passport resulted in 188 cases of refusal of passport services; 488 cases of revocation of passports; and 110 cases of individuals subject to periods of withheld services.

6.2.5 במסגרת ההיערכות לפני קבלת ההחלטות על בחירה במערכת זאת, בוצע ניסוי שתוצאותיו מתוארות במסמך

Cat. No. Ci4-2/2008E, ISBN 978-0-662-47667-2 : Biometric Field Trial



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

להלן טבלה מתוך הדו"ח המציגה מספר ממצאים:

Table 4-C: Interesting field trial facts

ITEM	VOLUME
Field trial clients claiming refugee status in Canada	12 ¹
Multiple enrolments (biometric matches)	394 • 182: only photos available for the repeat clients (mail-in applications, not seen in Vancouver) • 195: both photos and fingerprints available for the repeat clients • 17: only fingerprints available⁵
Number of clients who applied multiple times	364
Clients correctly matched using only facial recognition with system recommended threshold	98.4%
Clients correctly matched using only fingerprints with system recommended threshold	97.9%
Clients correctly matched using both facial and fingerprint recognition	100%

6.3 ניו - זילנד:

6.3.1 היישום בניו-זילנד מתואר בקישור הבא:

http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10845135

6.3.2 ניו-זילנד מפעילה מאגר תמונות שכולל כ- 4.5 מיליון תמונות. לקראת הפעלת המערכת בתצורה מקוונת לבקשה לחידוש דרכון, הוחלט לבצע טיוב נתונים ולבדוק קיומן של רשומות כפולות במערכת. לשם כך הופעלה מערכת לזיהוי פנים. כתוצאה מכך הוצפו כ- 210,000 חשודים, שנבדקו ידנית על ידי צוות מפעילים ובסופו של דבר נמצאו 65 חשודים בהרכשה כפולה מתוכם 30 הופנו לחקירת משטרה. חלק ניכר מההחשדות האחרות נגרם עקב תקלות פקידותיות. סה"כ בוצעו 21 טריליון בדיקות.

6.3.3 המאמר מצטט את מר דייוויד פילפ, המנהל האחראי במשרד הפנים על הנפקת הדרכונים.

6.3.4 כאן נראה אם כן שהשימוש אינו נעשה באופן שוטף, אלא בוצע למטרה מסוימת בנקודת זמן מסוימת.

6.4 יישומים שונים במדינות שונות בארה"ב בהקשר להנפקת רישיונות נהיגה:

6.4.1 ריכוז המדינות בארה"ב שבהן יש מאגרי תמונות פנים:

6.4.1.1 קישור:

<http://www.theblaze.com/stories/2013/06/17/say-cheese-some-states-put-drivers-license-photos-in-facial-recognition-database-for-law-enforcement-use/>

6.4.1.2 מאמר זה והקישורים דרכו, מצביעים על מצב שבו יש כיום בארה"ב ב- 37 מדינות (states) מאגרי מידע הכוללים כ- 120 מיליון אזרחים אמריקאים שמבקשים לקבל רישיון נהיגה, וכן non-driver's license, כך שרישיון הנהיגה משמש למעשה כמעין תעודת זהות.

כתובת לקבלת דואר, קפלן 3, הקריה, ירושלים 91919
שד' שאול המלך 8, תל אביב, טל: 03-7779222, פקס: 03-7779219



הממונה על היישומים הביومترיים

The Biometric Applications Commissioner

-בלמ"ס-

6.4.1.3 המאמרים השונים בקישור זה מציינים שב- 26 מתוך אותן 37 המדינות בהן יש מאגרי פנים, ניתנת גישה למשטרה לצורך חקירות.

6.4.2 מדינת אינדיאנה:

6.4.2.1 קישור:

<http://www.govtech.com/public-safety/Facial-Recognition-Helps-Indiana-Secure-Driver.html?page=1>

6.4.2.2 הדיווח הוא מ- 2009. מתואר בסיס נתונים של 6.5 מיליון תמונות (בוצע טיוב נתונים מ- 13 מיליון רשומות). ההערכה היא לתוספת של כ- 1.8 מיליון רישיונות לשנה. כלומר, כיום אמורים להיות במאגר כ- 15 מיליון תמונות.

6.4.2.3 צוין כי כ- 5% מהבקשות (כ- 500 ליום) נבדקות ידנית.

6.4.3 מדינת אילינוי:

6.4.3.1 קישור:

<http://www.govtech.com/public-safety/Biometrics-Stems-Driver-License-Fraud.html>

6.4.3.2 מצוין כי בין השנים 1997 – 2007 גילו כ- 5,000 מקרים של ניסיונות להרכשה כפולה, ביניהן 4,600 עם זהות כפולה אחת וכ- 600 עם יותר משתי זהויות.

6.4.4 מדינת ניו-יורק:

6.4.4.1 קישור למאמר בנושא "תעודת תושב של העיר ניו יורק":

<http://www.biometricupdate.com/201412/new-york-city-to-use-facial-recognition-software-for-municipal-id-program>

6.4.4.2 קישור להכרזת מושל ניו-יורק – איתור 13,000 מקרי זיוף תוך שימוש בזיהוי פנים:

<https://www.governor.ny.gov/news/governor-cuomo-announces-13000-identity-fraud-cases-investigated-dmv-using-facial-recognition>

6.4.4.3 קישור לנתונים שדווחו על ידי משטרת ניו-יורק בקשר ליחס שבין זיוף רישיונות נהיגה לבין המעורבות של אותם אנשים בתאונות דרכים ובעבירות אחרות:

http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2953&issue_id=62013

במאמר זה ישנו גם תיאור של התפתחות המערכת הכוללת כיום כ- 21 מיליון תמונות, כאשר בכל יום ניטלות כ- 7,000 תמונות חדשות ומושוות למאגר הכללי.

6.4.4.4 מאמר ממוקד בנושא זיוף רישיונות נהיגה (NY DMV):

http://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2013/2013_Regional_Conference/Tuesday_July_16/3%20-%20O.%20McShane%20-%20Region1%20Presentation.pdf

6.5 יישומים משטריים:

6.5.1 יישומים מבצעים עבור משטרות, המבוססים על זיהוי פנים, מופיעים במספר מקורות. מדובר בכלים ביצועיים שעליהם מסתמכים לצורך אכיפת החוק.

6.5.2 משטרת אוהיו, ארה"ב:

6.5.2.1 קישור לסרטון: <https://www.youtube.com/watch?v=XjvwJlqpFQI>

6.5.2.2 ר' בפרט דקות 4:00, 4:50, 6:30 בסרטון.

6.5.3 משטרת קלגרי, קנדה:

6.5.3.1 קישור:

כתובת לקבלת דואר, קפלן 3, הקריה, ירושלים 91919
שד' שאול המלך 8, תל אביב, טל: 03-7779222, פקס: 03-7779219



הממונה על היישומים הביומטריים

The Biometric Applications Commissioner

-בלמ"ס-

<http://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1.2822592>

6.5.3.2 מדובר על מערכת חדשה יחסית, שהותקנה בנובמבר 2014. צוין שם שזאת המשטרה הראשונה בקנדה העושה שימוש במערכת.