סייבר ישראל
מערך הסייבר הלאומי

זיהוי פנים במרחב הציבורי

המכון הישראלי למדיניות הטכנולוגיה

נעמה בן צבי

ראש מרכז פיקוח והכוונה
היחידה להזדהות ויישומים ביומטריים
מערך הסייבר הלאומי
naamab@cyber.gov.il

נובמבר 2022

היחידה להזדהות ולייושמים ביומטריים - תחומי פעילות

פיקוח על פרויקט תיעוד לאומי חכם

יישומים ביומטריים

הזדהות בטוחה

מעבדה ביומטרית לאומית

שומר זה"ב

זיהוי פנים במרחב הציבורי

תפיסה כוללת לשימוש בביומטריה במעברי גבול

קידום מחקר ופיתוח

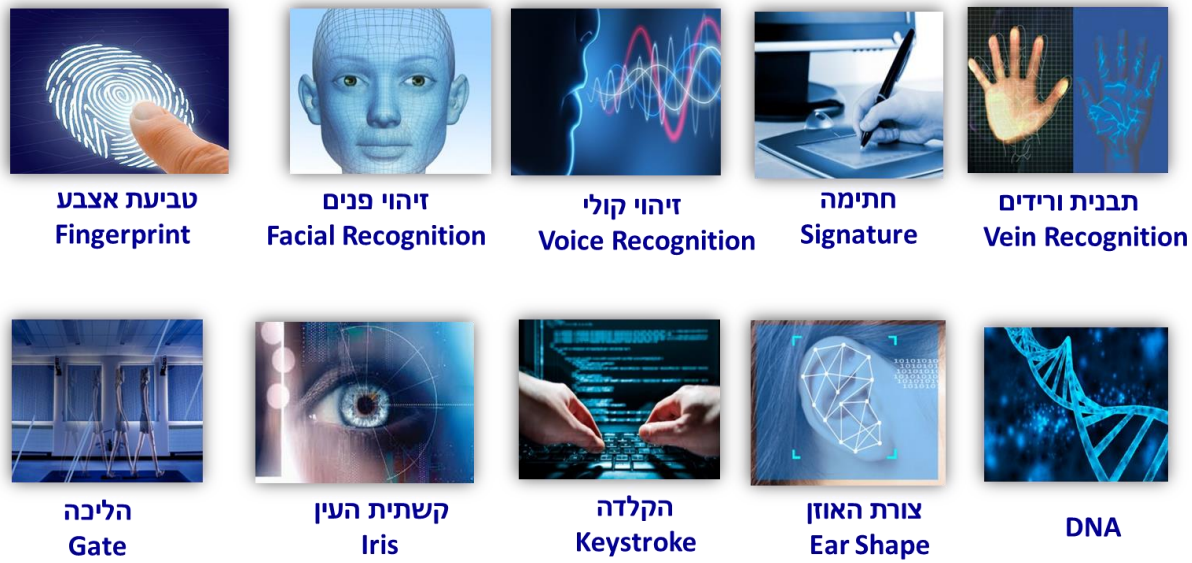
?

מהו אימות ביומטרי, מהי ביומטריה

<u>בתכונה</u> - מאפיין ביולוגי (אנטומי או פיזיולוגי) והתנהגותי הניתן למדידה, אשר ניתן לעשות בו שימוש לזיהוי אוטומטי

<u>בתהליך</u> - שיטות אוטומטיות של זיהוי אדם בהתבסס על מאפיינים ביולוגיים (אנטומיים ופיזיולוגיים) והתנהגותיים ברי מדידה

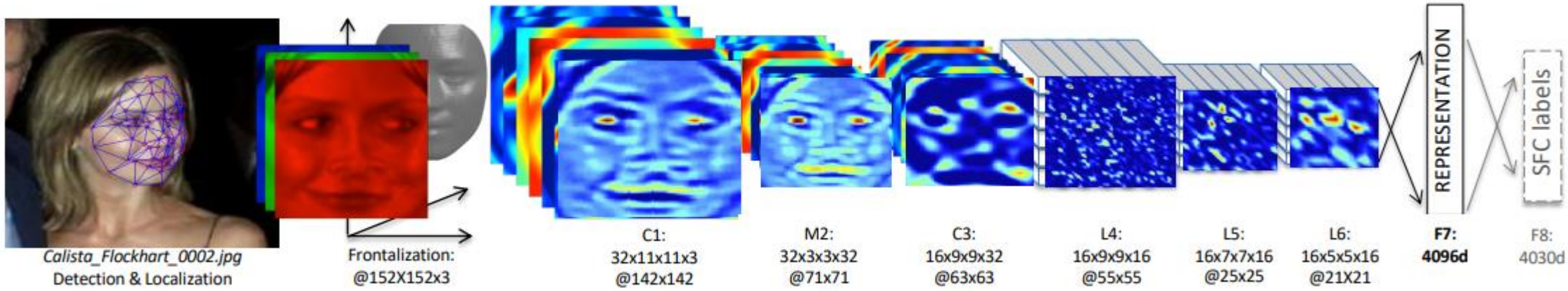
»»» סוגי ביומטריה



דיגום ביומטריה

- זיהוי פנים: זיהוי של בני אדם ע"פ מאפיין ביולוגי
- אני יודע להבחין בין אנשים שונים, ואני יודע לזהות אדם שזיהיתי בעבר
- עצם פעולת הזיהוי האנושי היא זיהוי ביומטרי
- עצם הצילום, למשל במצלמות אבטחה, כבר מהווה "דיגום ביומטרי"

«««« ביומטריה ממוחשבת-בינה מלאכותית - DCNN



Y. Taigman, M. Yang, M. Ranzato, L. Wolf. **DeepFace: Closing the Gap to Human-Level Performance in Face Verification.**
IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2014.

זיהוי- IDENTIFICATION

חיפוש במאגר 1:M

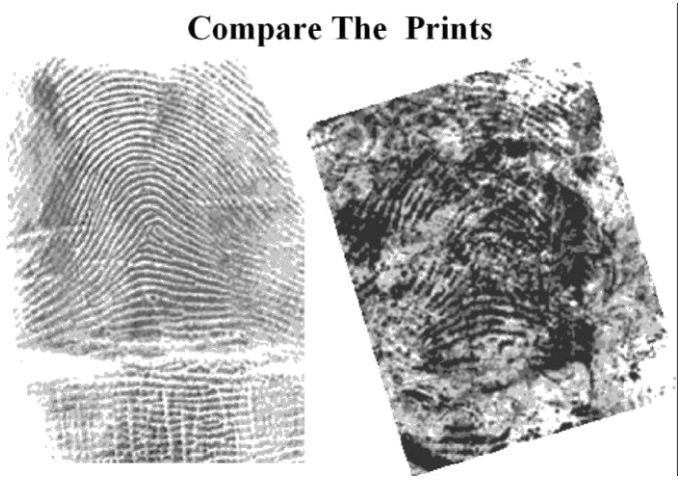
- במאגר המשטרתי
  – דגימות שניטלות מאדם / זירה
- מאגר להנפקת תיעוד לאומי
  - מניעת "הרכשות בפולות"
- מול watchlist- בדיקה ביטחונית, מרחב ציבורי

אימות- VERIFICATION

בדיקה מול רשומה 1:1 (מאגר/device)

- במעבר הגבול- בדיקה מול הרשומה שבדרכון
- ב"פתיחת הסלולארי"- בדיקה מול הרשומה שבמכשיר
- מערכות בקרת כניסה/נוכחות (חלק מהמערכות)

ביומטריה והסתברויות



- כל ביומטריה מועדת לשגיאות
- כל מדידה מניבה "ציון התאמה"

= הסיכוי להתאמה, בין 0% ל-100%

- שיטות שונות לתפעול מערכת

סייבר ישראל
מערך הסייבר הלאומי

ביצועים של מערכות ביומטריות

"קצב השגיאות"

FRR/FNIR המערכת "דוחה" את הטענה שהדגימה של אדם א' תואמת לדגימה אחרת שלו, למרות שזו שגיאה

FAR/FPIR: המערכת "מקבלת" את הדגימה של אדם א' בתואמת לדגימה של אדם ב', למרות שזו שגיאה

FTA: כישלון בהרכשת הביומטריה

זיהוי פנים במרחב הציבורי- איך זה נראה

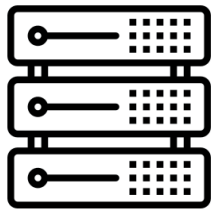
Face recognition “in the wild” of non-cooperative subjects

מערכות מבוקרות (השוואה ביומטרית בסלולאר/בקיוסקים/בקרת כניסה)

ארכיטקטורה כללית

CCTV cameras

Body-worn cameras



Processing servers (distributed architecture)

Cloud or on premises

Central management nodes

Database, storage and API

Dashboards

Controlled Live Portrait Photos

Face Recognition Vendor Test (FRVT)
Part 2: Identification

FPIR/FNIR - 1% ⬇

Faces In The Wild

Face In Video Evaluation (FIVE)
Face Recognition of Non-Cooperative Subjects 2017

שיעורי השגיאה?

אתגרים

תאורה

ללא
שיתוף פעולה

זוויות צילום

מזג אויר

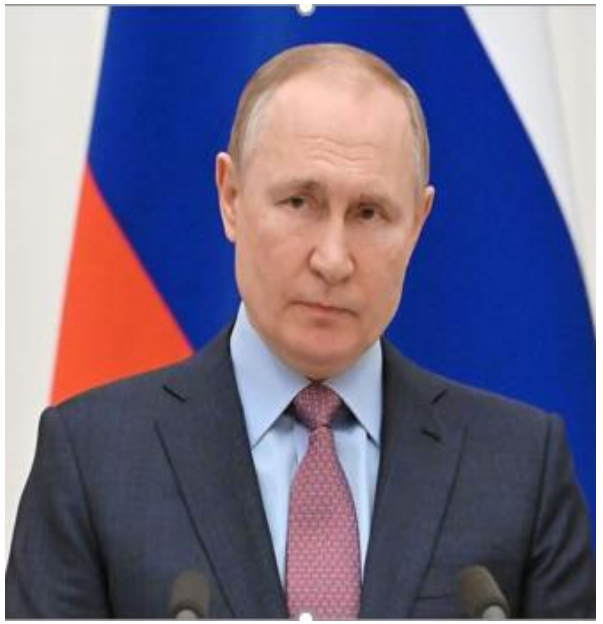
כיסויים

»»» זיהוי פנים- מערכות לא מבוקרות (הדגמה 1:1)

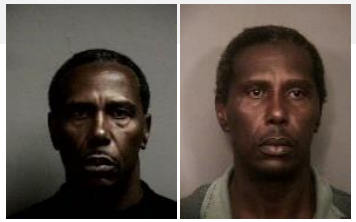
ALGO1:8603 success
ALGO2:88 success
ALGO3:0.87 success

ALGO1:5967 falied
ALGO2:- Error
ALGO3:0.78 success

ALGO1:5960 falied
ALGO2:0 falied
ALGO3:0.76 success

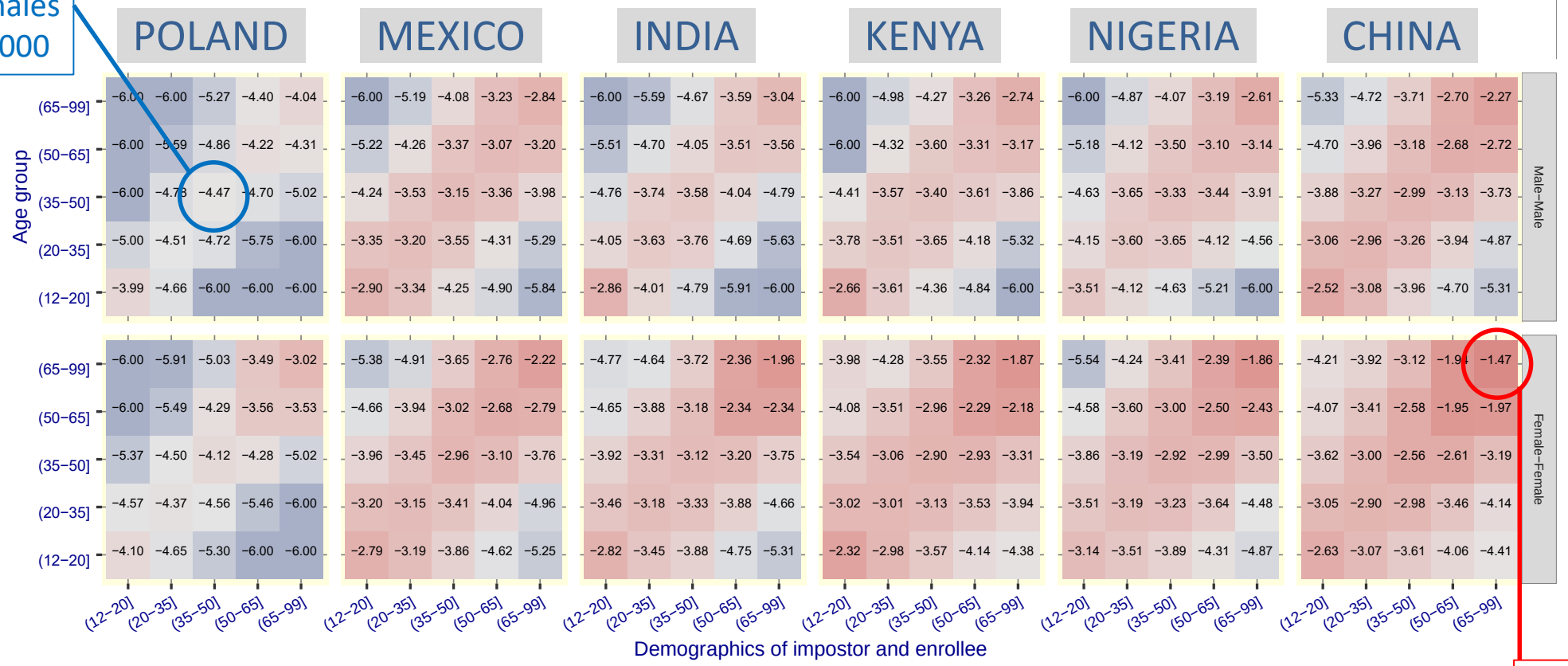


Demographics: Two classes of demographic effect

1. # people	2. Example photos	3. Name of error	4. Cause of error	5. Who is affected?	6. Mitigation
1 person		False Negative	Poor photography and algorithm intolerance of it.	1. Underexposure of dark skin, reduces information 2. Tall or short people, with fixed height camera, gives head pose “pitch” problem	1. Fix photography 2. Use a more accurate algorithm
2 persons		False Positive	Algorithm response, occurs even with pristine images	1. In the young 2. In women 3. In ethnicities “unknown” to the algorithm 4. Generally: In groups that are under-represented in the training data.	1. Replace the algorithm with a new edition 2. Raise the threshold to suppress false positives in the most affected demographic

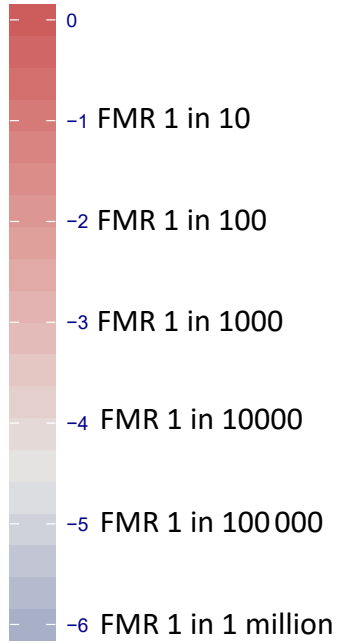
Magnitude matters: Age x Age for six countries

FMR on Polish males 1 in 30 000



Algorithm: imperial_002
Threshold: 1.381120
Dataset: Application
Nominal FMR: 0.000030

log10 FMR



Summary Stat. #1:	Maximum / Minimum	~ 1000
Summary Stat. #2:	Maximum / Geometric Mean:	~ 43

FMR ~ 1 in 30 on Chinese women > 65

סיכונים

שגיאות

60 MINUTES

פרטיות


The laser beams can disorient police and block facial recognition technology CREDIT: SIPA USA

The Telegraph

סייבר

Forbes

Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked

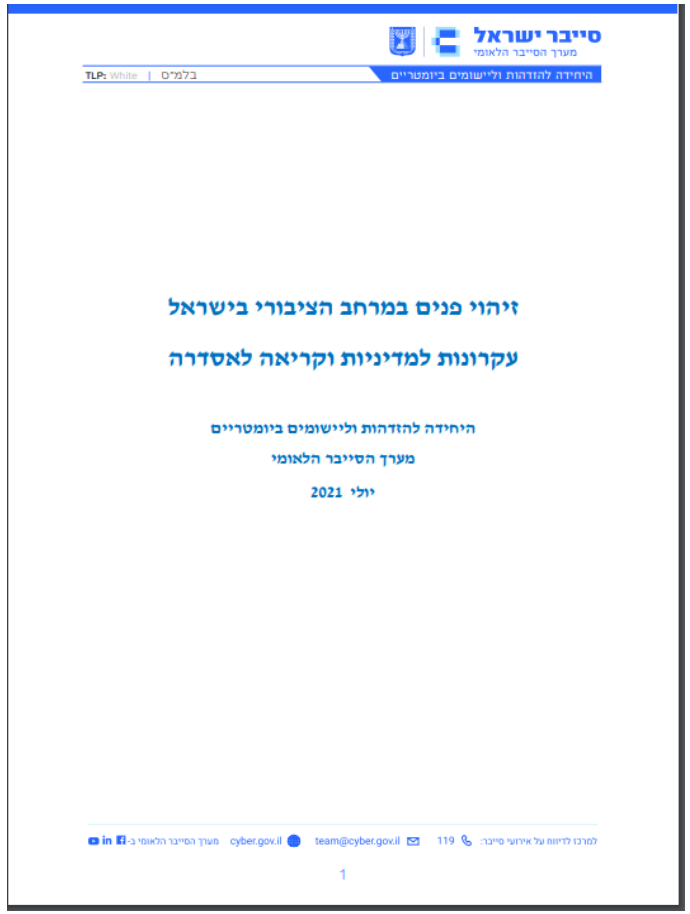
it governance

How worried should you be by the BioStar 2 breach that leaked 1 million people's biometric data?

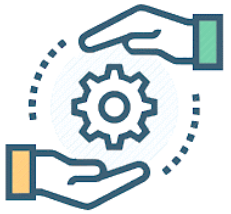
יוזמות רגולציה/מדיניות

Biometrics and Surveillance Camera Commissioner

11 עקרונות מדיניות (אחריות ניהולית וטכנולוגיה, הגנת הסייבר, פרטיות ואתיקה)



לגיטימיות המטרה



תקינות המערכת

פיקוח ובקרה

תזכיר חוק לתיקון פקודת המשטרה [נוסח חדש] (תיקון מס') מערכות צילום מיוחדות התשפ"א 2021

שימוש לא אתי בהגדרת מוכללים

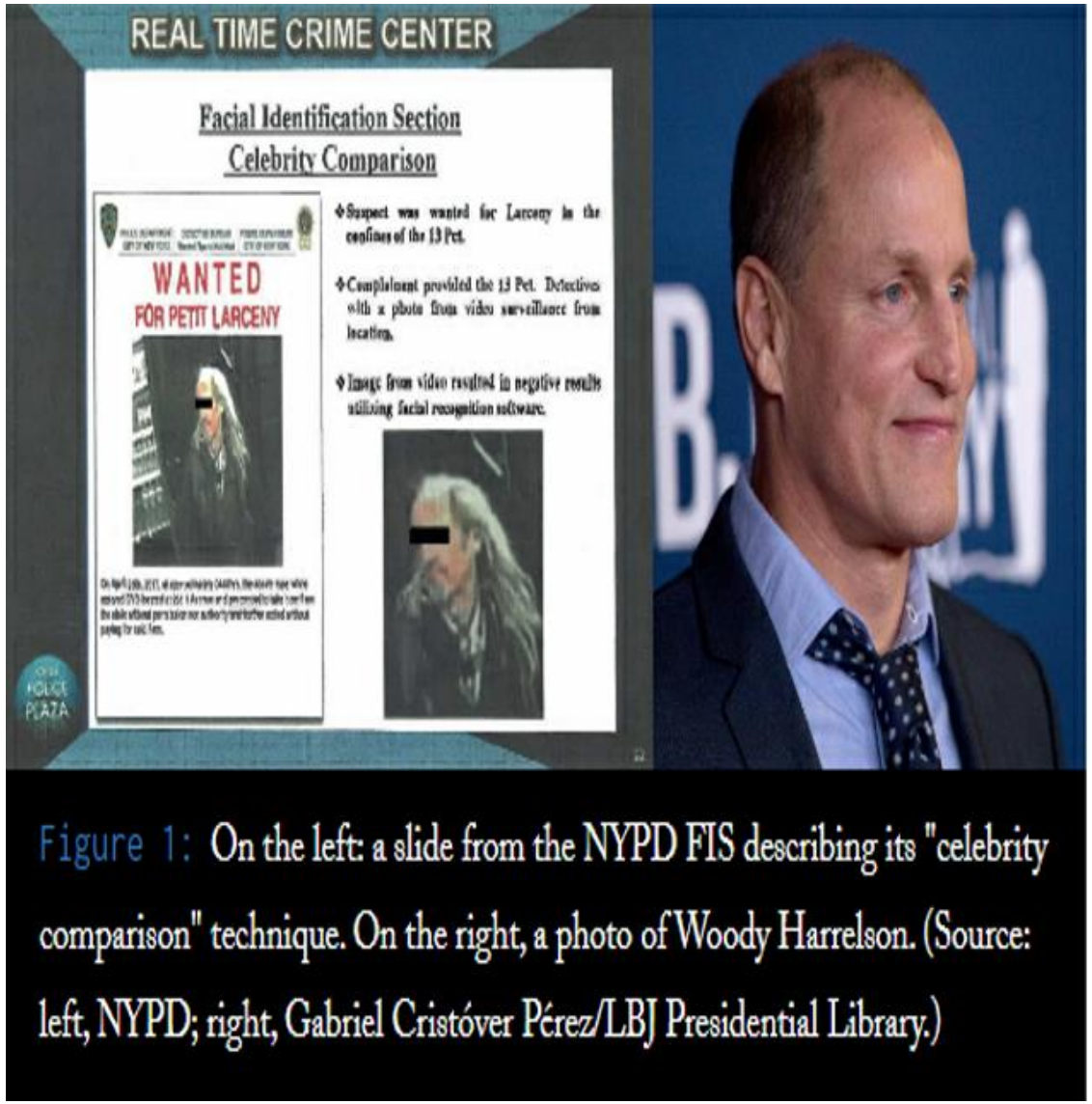


Figure 1: On the left: a slide from the NYPD FIS describing its "celebrity comparison" technique. On the right, a photo of Woody Harrelson. (Source: left, NYPD; right, Gabriel Cristóver Pérez/LBJ Presidential Library.)

סייבר ישראל
מערך הסייבר הלאומי

תודה על ההקשבה