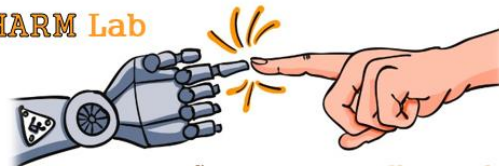




חשיפה למחקר המחלקה להנדסת תעשייה וניהול

רון הירשפרונג



ה"פילוסופיה" שמאחורי המוטיבציה המחקרית

❖ פרטיות היא סוגייה מרכזית,
ונחשבת בעולם המערבי ל-
Human Right.

❖ אדם אינו יכול להזיז אבן
כבדה שהונחה במקום מסוים
ע"י מכונה.
להשגת מטרה זו הוא נדרש
להשתמש בשירותיה של
מכונה אחרת.



❖ כמשל: כיוון שהפרטיות מופרת בעיקר ע"י מכונות (AI) ⇔
נדרש שימוש בעוצמה זהה, קרי AI, לשמירת הפרטיות.

❖ ניתן להגיד שהמחקרים שלי עוסקים ב:

Harnessing AI to defeat AI



הגנת פרטיות פרואקטיבית

[illegible]

Sponsored

מחפץ לכלב מזה...
מיטה לכלב דורה, ספר
מזון אוטומטי עבה
\$29.77
AliExpress

מיטה לכלב Dog bed
דורה, קנה חית מתמיד
משוף ורחיץ בגודל ...
\$70.17
Temu

מיטה כלבים דורה
אורטופדית, מיטה
כלבים לנכים גדולים ...
\$56.04
Temu

oop Pets Project
פארקט מזון דחה חים
לכלב (L)
\$229.00
All4Pet

oop פארקט מזון
פרומו דחה חים
לכלב 110*70*5
\$129.00
ikatan

מזריות לנכים עם
הסגן, מזריות משולפת
מזריות
כלבים לשנה...
\$45.07
AliExpress

Sponsored

temu.com
<https://www.temu.com>

Temu מכירת חיטיל - מזון לכלב - Temu

דיעה ממזון לכלב ב-חשוד רשות ביתר, אינת זישת מן הכלל זמנן מאל של שירותים של טעמו. מזון לכלב מדויקים
אינת גבוהה ב-Temu.
גדיר גבריי: איהל לקוח - כל המכשפים : מיקום תונת : מזון לכלב מבוצע : מזון לרל קדרשה יצרן

Sponsored

AliExpress
<https://www.aliexpress.com>

לכלב מיטה Pet Bed - AliExpress

Low prices in electronics, women's and men's fashion, home appliances. Smarter online...

★★★★★ Rating for aliexpress.com: 4.5 - 363 reviews

AnimalShop.co.il
<https://www.animalshop.co.il> · [Translate this page](#)

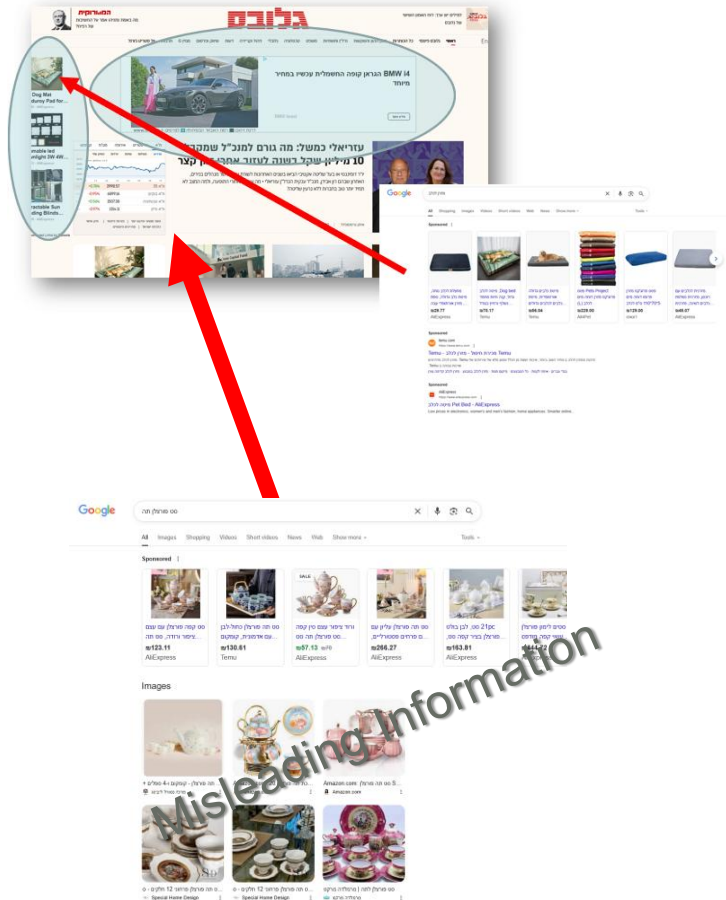
מיטה לכלב - מחירים פצצה מגוון עקב

מזון לכלב שווה יותר, על לשינוע נוסח לפריסה וגם ברירה או על שושן רק. מהר עשויות מיטות להיכליל היחסות



הגנת פרטיות פרואקטיבית

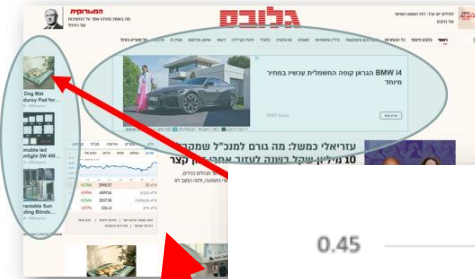
❖ פתרון אפשרי: Anonymization



CONTROL



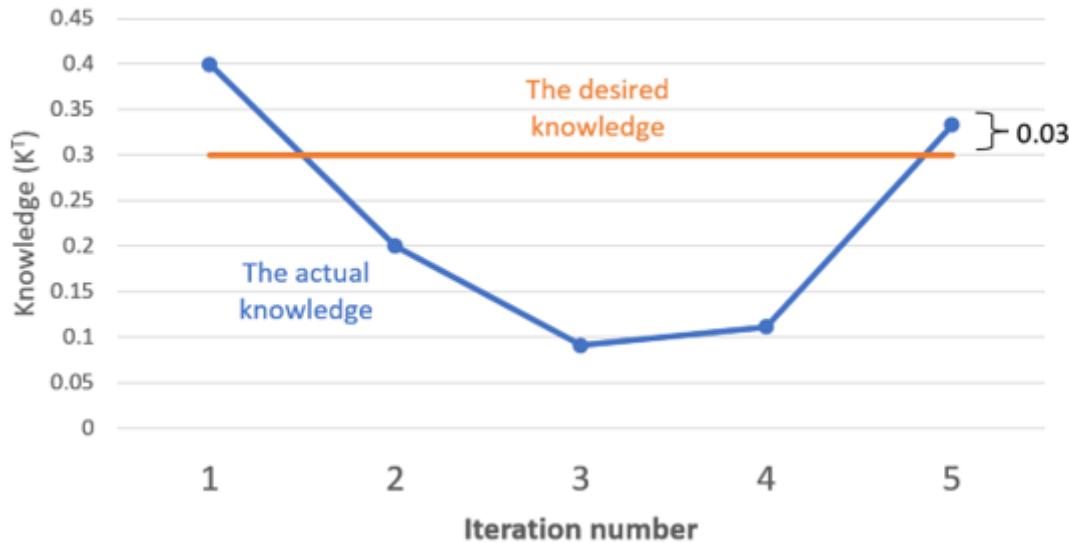
הגנת פרטיות פרואקטיבית



Algorithm 1:

Single Iterations Cycle – a set of iterations of searching and browsing with the same p^r

// decide if search is performed on S^r (real) or S^m (Misleading)



end repeat

We define the transfer function given the input p_{l-1}^r (the $(K^T$ received after the last cycle), as:

$$p_l^r = p_{l-1}^r + \frac{K^{des} - K^T}{s}$$

$$K^T = \frac{|A^r|}{|A^r| + |A^{om+}| + |A^{om-}|}$$

while $|K^T - K^{desT}| > TR$
 $p^r = p^r + \frac{K^{desT} - K^T}{step}$
run Single Iterations Cycle
end while

external process

utilization

P_{first}
 $Initial_DecayFactor$
 P_{rem}

Iterations Cycle

– evaluate knowledge()



“Adon Olam”

<https://www.youtube.com/embed/d29qSLUstxw?enablejsapi=1&wmode=opaque&autoplay=0>



Makes me happy on many levels - the soulful, minor melody of the verses moves to an upbeat major chorus of hope and appreciation; the words can fit almost any other melody; reminds me of great times with my kids and at shul

Musical features

- YouTube ID extraction
- SOPTIFY API

danceability	0.438
acousticness	0.763
energy	0.382
instrumentalness	0.00301
liveness	0.112
loudness	-9.3
speechiness	0.0288
tempo	149.967
valence	0.185
key	9
mode	0

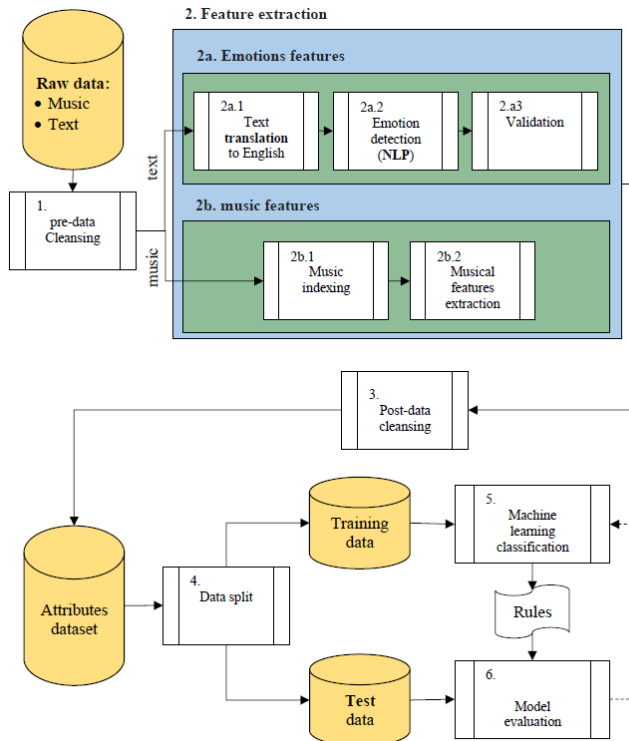
anger	0.000956
disgust	0.000689
fear	0.000212
joy	0.98506
neutral	0.005446
sadness	0.00452
surprise	0.003117

Emotions

- text translation
- NLP (DistilRoBERTa)
- Manual validation



מוזיקה כמזהה אישי



- First emotion prediction:

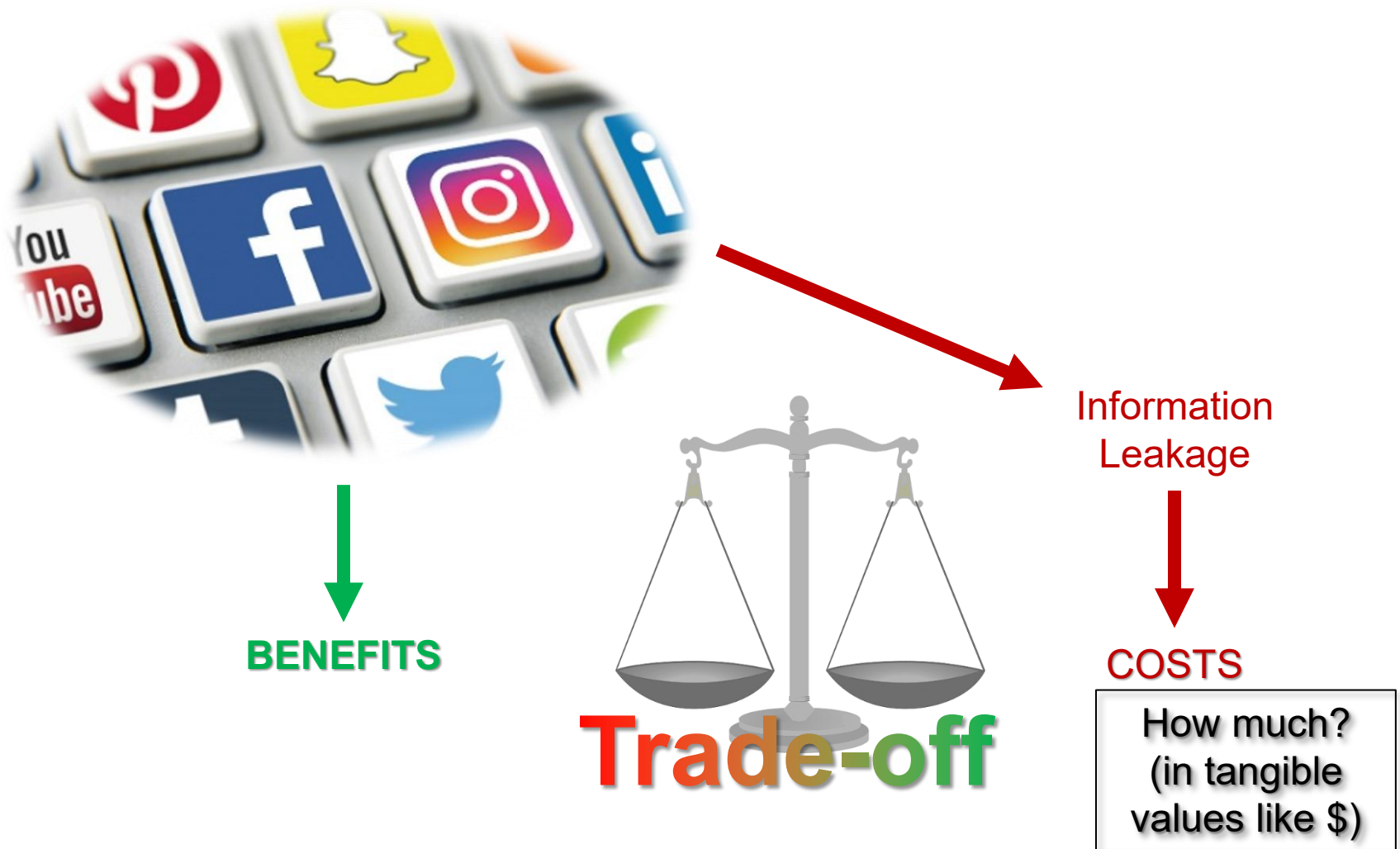
$$\text{Accuracy} = 0.575 \text{ (baseline} = \frac{1}{7} = \sim 14.3\%)$$

- One of the two leading emotions prediction:

$$\text{Accuracy} = 0.751 \text{ (baseline} = \frac{12}{42} = \sim 28.6\%)$$



ערך זליגת מידע ברשתות חברתיות



ערך זליגת מידע ברשתות חברתיות



You are ab

You can get a
if you agree that your Bank ac

Notation	Description
PL	Platform: the factor of which kind of platform (OSN) is the exposure on
SI	Sell Item: the factor of the item being sold
DI	Data Item: the factor of what kind of personal data is exposed in the network
$v_{i,j}$	Initial value of offering for $i = PL, j = DI$
$R_{i,j}$	Random choice for $i = PL, j = DI$
$accepted$	Boolean, the participant accepted/not accepted the offer.
$during$	Boolean, at what stage of the purchase the discount is given.
$t_{i,j}$	number of times the offering will be suggested- to set upper and lower bounds.
Δ_{max}	maximal value increase offered to participants.
Δ_{min}	minimal value decrease offered to participants.
$price_{accepted}$	the price the user accepted for the risk of his data leaking
B_{upper}	upper bound of estimated value of privacy
B_{lower}	lower bound of estimated value of privacy
R_t	random int (0-3) for a minimal 0 times and maximal 3 times of increasing/decreasing offer

The evaluation method

After defining the notation and the matrix of values for the different factors we proceed to define the game's algorithm, that is as follows:

Algorithm 1. PrivacyValueEstimationGame

input: $v_{i,j}$, $accepted$, $during$, $t_{i,j}$, Δ_{max} , Δ_{min} , $price_{accepted}$, B_{upper} , B_{lower} , R_t
 $B_{lower} \leftarrow 0$
 $B_{upper} \leftarrow \infty$
 $price_{accepted} \leftarrow 0$
 $accepted \leftarrow false$
 if $during = false$
 for all the values of SI
 $R_{i,j} \leftarrow$ Random value from the cells $c_{i,j}$ from Matrix $(PL \times DI)$
 Offer a coupon with the value of $v_{i,j}$
 if $accepted = true$
 $price_{accepted} \leftarrow v_{i,j}$
 $B_{upper} \leftarrow price_{accepted}$
 end if
 else
 $B_{lower} \leftarrow v_{i,j}$
 $B_{upper} \leftarrow v_{i,j} + \Delta_{max}$

```

end else
end if
for all the values of  $SI$ 
 $R_{i,j} \leftarrow$  Random value from the cells  $c_{i,j}$  from Matrix  $(PL \times DI)$ 
Offer a coupon with the value of  $v_{i,j}$ 
if  $accepted = true$ 
   $price_{accepted} \leftarrow v_{i,j}$ 
   $B_{upper} \leftarrow price_{accepted}$ 
   $t_{i,j} \leftarrow R$ 
   $index \leftarrow 0$ 
  while  $index < t_{i,j}$ 
    Offer  $v_{i,j} - \frac{index}{t_{i,j}} \Delta_{min}$ 
    if  $accepted = false$ :
       $B_{lower} \leftarrow price_{accepted}$ 
    end if
    else
       $price_{accepted} \leftarrow v_{i,j}$ 
    end else
     $index \leftarrow index + 1$ 
  end while
end if
else
   $B_{lower} \leftarrow v_{i,j}$ 
   $B_{upper} \leftarrow v_{i,j} + \Delta_{max}$ 
   $t_{i,j} \leftarrow R$ 
   $index \leftarrow 0$ 
  while  $index < t_{i,j}$ 
    Offer  $v_{i,j} + \frac{index}{t_{i,j}} \Delta_{max}$ 
    if  $accepted = true$ 
       $price_{accepted} \leftarrow v_{i,j} + \frac{index}{t_{i,j}} \Delta_{max}$ 
       $B_{upper} \leftarrow price_{accepted}$ 
    end if
     $index \leftarrow index + 1$ 
  end while
end else
end for
return  $B_{lower}, B_{upper}$ 

```



ערך זליגת מידע ברשתות חברתיות

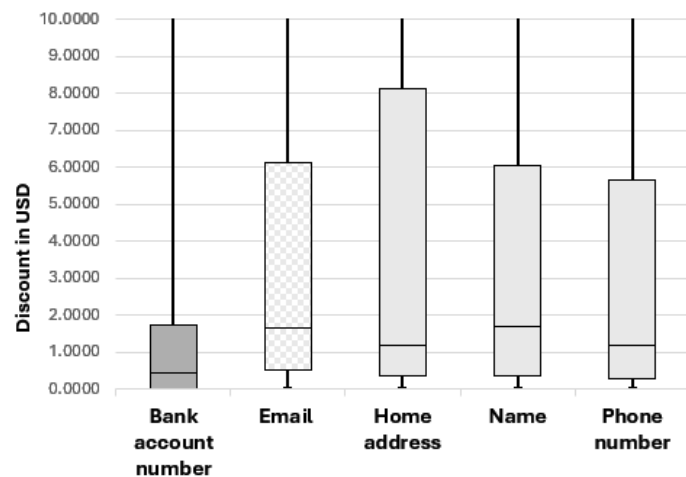


Figure 4. Box Plot results for types of personal data items.

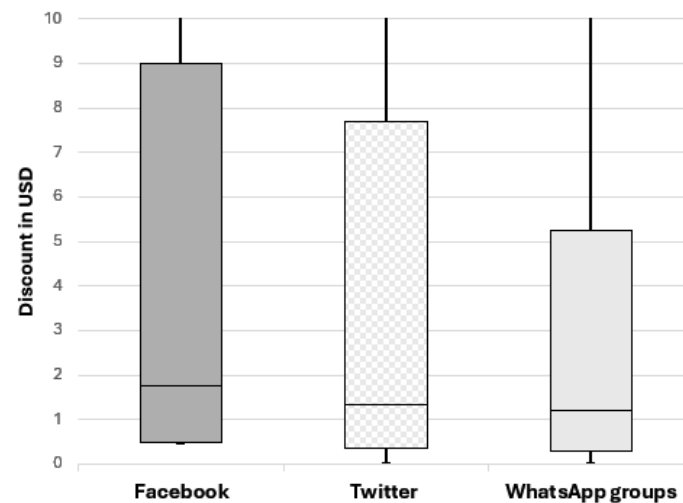


Figure 5. Box Plot results for types of platforms the data is exposed in.



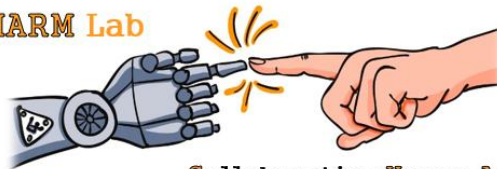


רון הירשפרונג



Ariel Cyber
Innovation
Center

CHARM Lab



Collaborative Human-Agent
Relationship Management

אוניברסיטת
אריאל
בשומרון