

# VirtualIdentity: a Privacy-Preserving User Profiling Service

Sisi Wang

[sisiwang@uw.edu](mailto:sisiwang@uw.edu)

M.S. in Computer Science

Faculty Advisors:

Dr. Martine De Cock & Dr. Anderson Nascimento

**The Secure ML team:**

Wing-Sea Poon, Golnoosh Farnadi, Caleb Horst,

Kebara Thompson, Michael Nickels, Chris Allan Vishoot & Such Kamal

<http://secureml.insttech.washington.edu/>

UNIVERSITY of WASHINGTON | TACOMA

Institute of Technology

SORT ▾

**American Express**

Taking advantage of post-holiday sales? Use Membership Rewards points for Mobile Gift Cards to select retailers right on your smartphone! <http://aexp.co/ruY>

AMERICAN EXPRESS

MEMBERSHIP REWARDS\*

POINTS AVAILABLE  
999,999

WILLIAMS-SONOMA

NEW!  
MOBILE GIFT CARDS

IN WALLET

BANANA REPUBLIC

GAP

SAN FRANCISCO, CA  
4023 6 000 000

Browse Mobile Gift Cards >

View Your Gift Card Wallet (4) >

Like · Comment · Share · 4,014 53 115 · Sponsored

Sponsored

Create an Ad



**American Express**  
Taking advantage of post-holiday sales? Use Membership Rewards points for Mobile Gift Card...



4,014 53 115

**Fresno All Laser LASIK**  
[fresnolasikeyesurgery.com](http://fresnolasikeyesurgery.com)



With LASIK, you won't have to worry about painful surgery or lengthy recovery times.

**Meet Singles On Facebook**

Interested Single Women. Sign up and see pics on Facebook. It's 100% free to look!

**Free Cab Fare For A Year!**

Share your safe alternative to driving

# User Profiling



## Machine Learning

Gender, Age,  
Personality,  
Religion, Sexual  
Orientation,  
Interest,...



*"On the Internet, nobody knows you're a dog."*

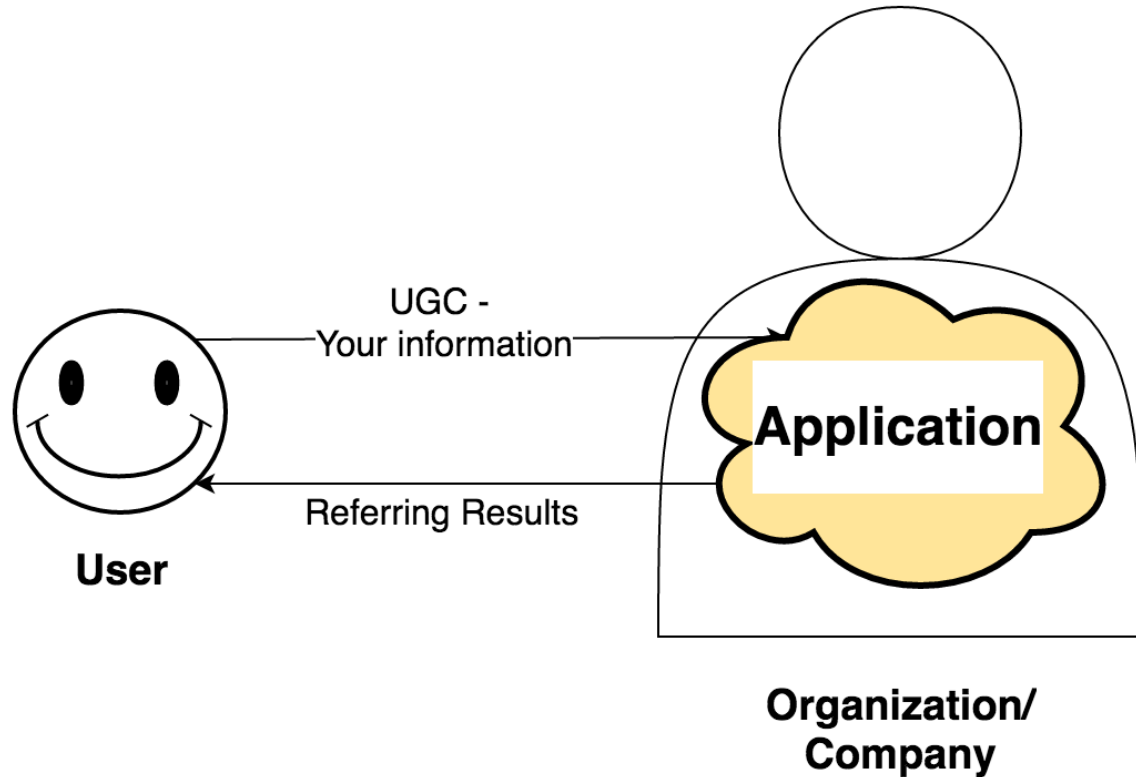
*Image Credit: The New Yorker cartoon modified by Eric Blattberg / VentureBeat*



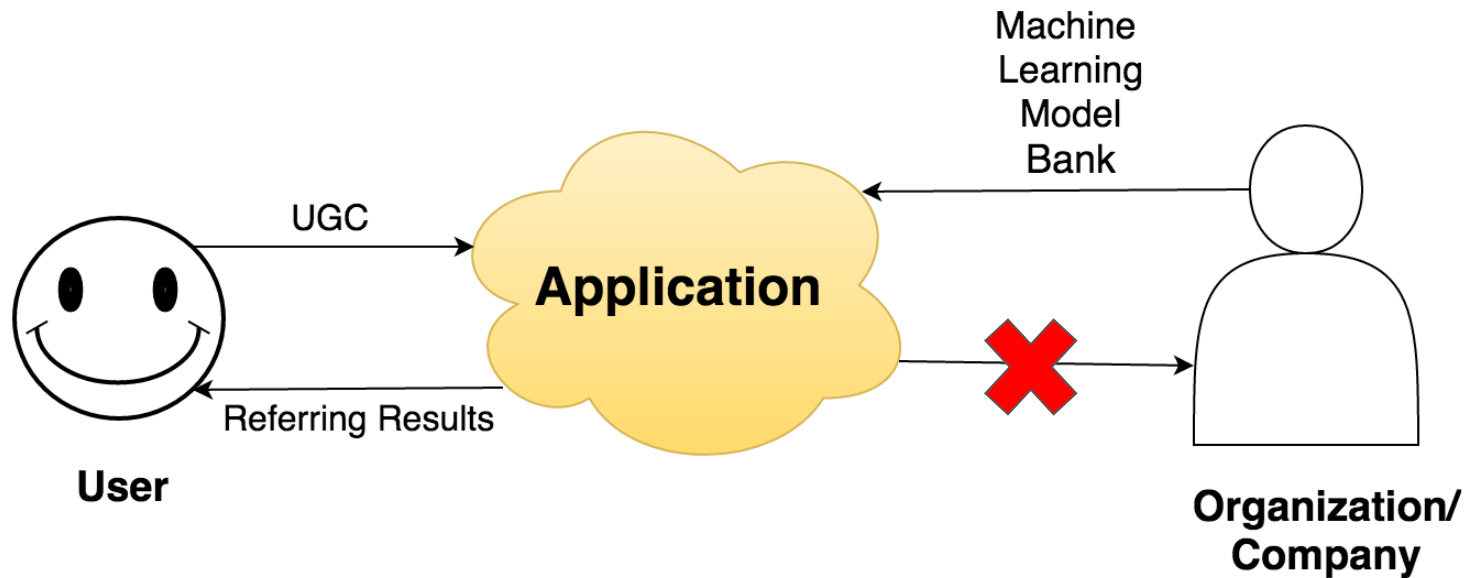


KDNuggets.com • cartertoons.com

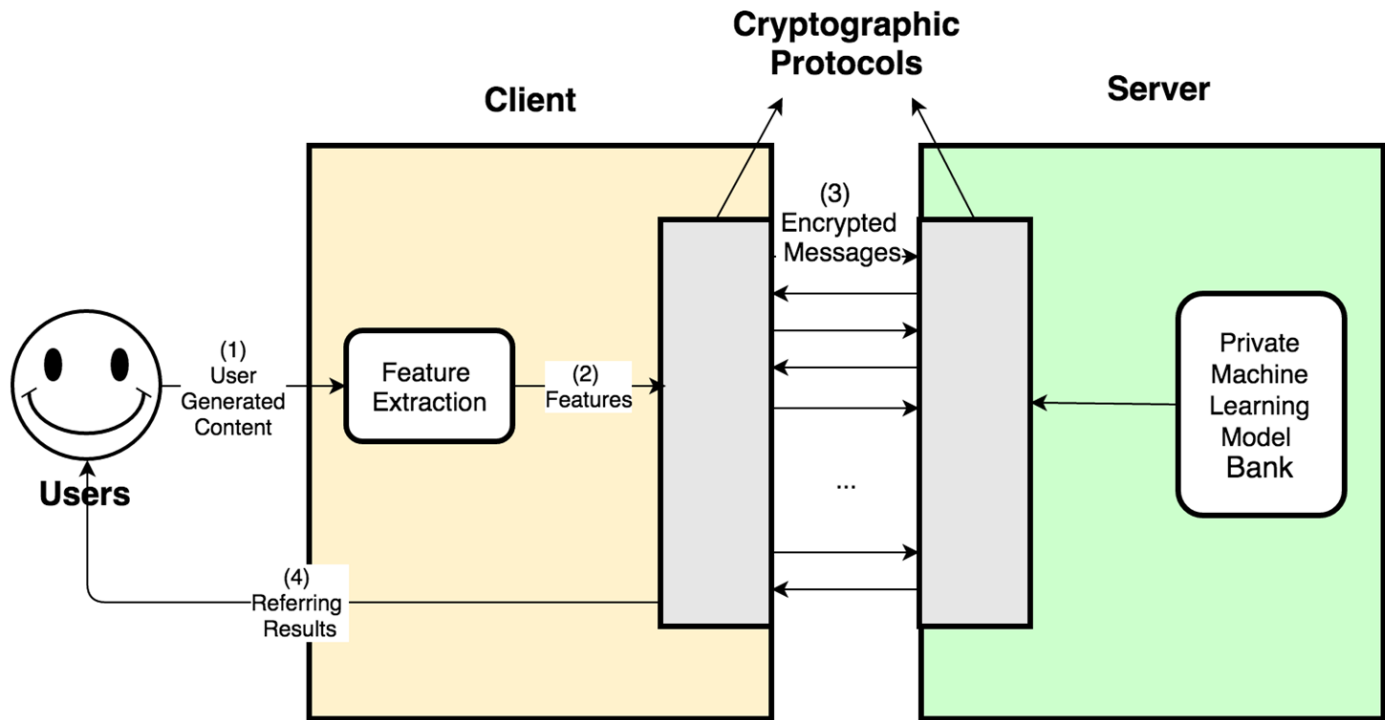
# Problem?



# Privacy-Preserving

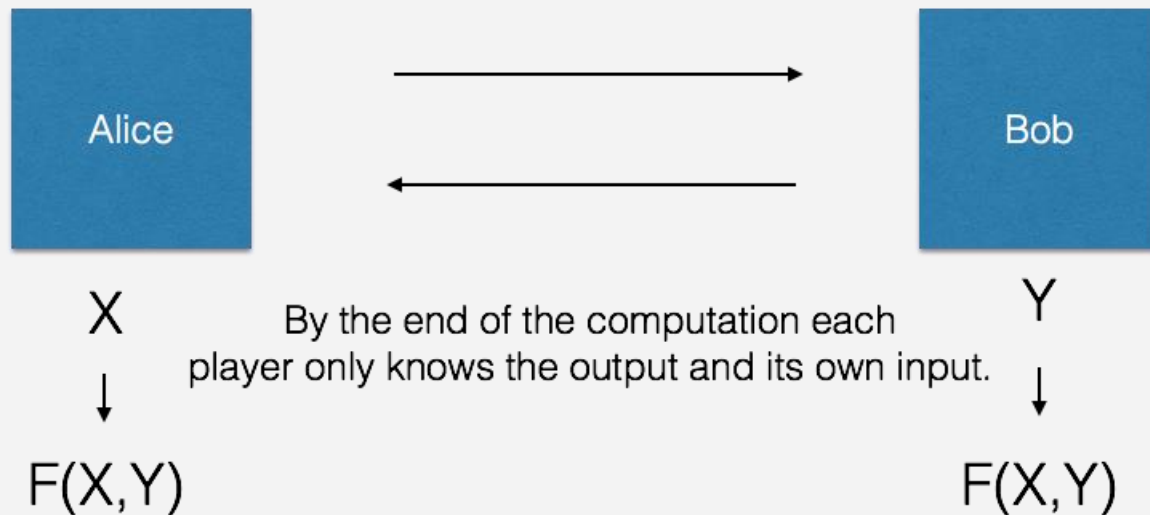


# VirtualIdentity -- Overview






# Secure Two Party Computations



**A. Yao. How to Generate and Exchange Secrets. In 27th FOCS, pages 162–167, 1986.**

# Cryptographic Protocols

Decompose **Machine Learning Scoring** operation  
into smaller and simpler operations



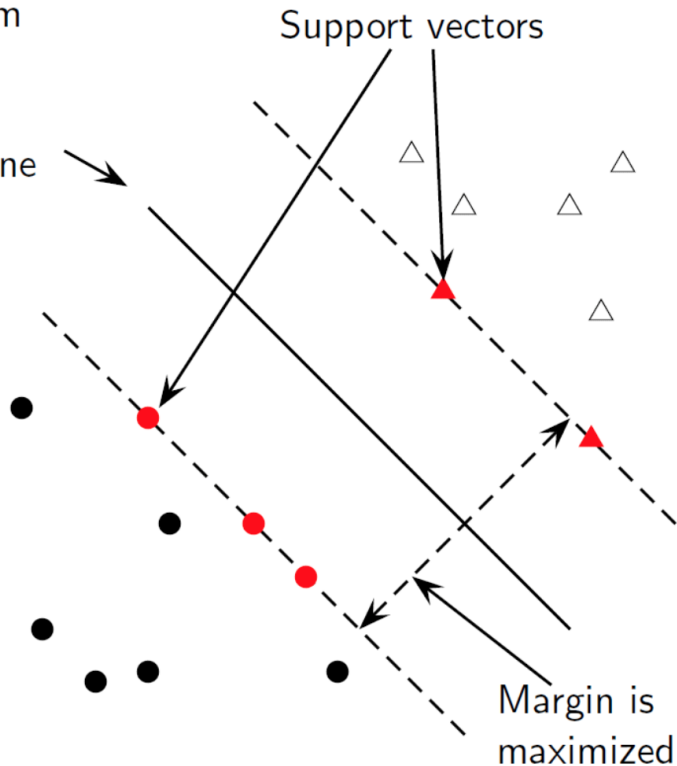
Use **Secure Multi-party Computation** to make each  
simple operation privacy-preserving



Combine the Secure Multi-party computations to get  
the Machine Learning Scoring privacy-preserving

# Support Vector Machine Scoring

Maximum  
margin  
decision  
hyperplane



Scoring for new instance  $x_q$ :

$$f(x_q) = \text{sign} \left( \sum_i \alpha_i y_i K(x_q, x_i) \right)$$

- Multiplication
- Addition
- Comparison
- ...

# Privacy-Preserving Comparison

## -- by Multi-party Computation

Let  $\ell$  be the bit length of the integers to be compared. The trusted initializer pre-distributes the correlated randomness necessary for the execution of all instances of the distributed multiplication protocol. The parties have as inputs shares  $\llbracket x_i \rrbracket_2$  of each bit of  $x$  and shares  $\llbracket y_i \rrbracket_2$  of each bit of  $y$ . The protocol proceeds as follows:

1. For  $i = 1, \dots, \ell$ , compute  $\llbracket d_i \rrbracket_2 \leftarrow \llbracket y_i \rrbracket_2 (1 - \llbracket x_i \rrbracket_2)$  using the multiplication protocol  $\pi_{DM}$  and locally compute  $\llbracket e_i \rrbracket_2 \leftarrow \llbracket x_i \rrbracket_2 + \llbracket y_i \rrbracket_2 + 1$ .
2. For  $i = 1, \dots, \ell$ , compute  $\llbracket c_i \rrbracket_2 \leftarrow \llbracket d_i \rrbracket_2 \prod_{j=i+1}^{\ell} \llbracket e_j \rrbracket_2$  using the multiplication protocol  $\pi_{DM}$ .
3. Compute  $\llbracket w \rrbracket_2 \leftarrow 1 + \sum_{i=1}^{\ell} \llbracket c_i \rrbracket_2$  locally.

**We hope to achieve highly practical results that  
allow the benefits of machine learning to be  
unlocked without the cost of individual privacy.**

**Check our website:** <http://secureml.insttech.washington.edu/>

Sisi Wang

M.S. in Computer Science

[sisiwang@uw.edu](mailto:sisiwang@uw.edu)

UNIVERSITY of WASHINGTON | TACOMA

Institute of Technology