DESIGNING MACHINE LEARNING

A Multi-Disciplinary Approach

Ethical Considerations

In Designing ML

What if machines become conscious?

Who is responsible when an algorithm commits crime?

How do I “appeal” an algorithm’s decision?

Will behavioral prediction erode my freedom to decide?

Ethical Considerations
In Designing ML

Will machines lead to mass unemployment?

Will machine systems become powerful surveillance tools?

How do you govern a multi-territorial computational system?

Will machine learning reinforce bias and discrimination?

d.ML

Robust De-anonymization of Large Sparse Datasets

Arvind Narayanan and Vitaly Shmatikov
The University of Texas at Austin

Abstract

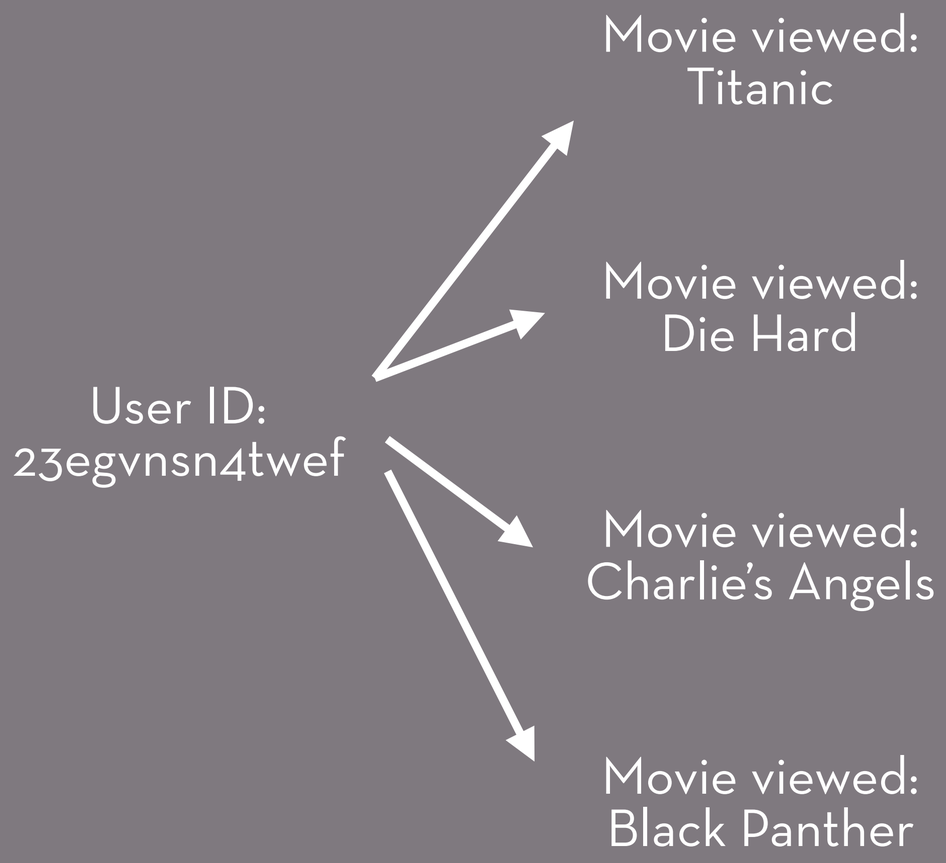
We present a new class of statistical de-anonymization attacks against high-dimensional micro-data, such as individual preferences, recommendations, transaction records and so on. Our techniques are robust to perturbation in the data and tolerate some mistakes in the adversary's background knowledge.

We apply our de-anonymization methodology to the Netflix Prize dataset, which contains anonymous movie

and sparsity. Each record contains many attributes (*i.e.*, columns in a database schema), which can be viewed as dimensions. Sparsity means that for the average record, there are no "similar" records in the multi-dimensional space defined by the attributes. This sparsity is empirically well-established [7, 4, 19] and related to the "fat tail" phenomenon: individual transaction and preference records tend to include statistically rare attributes.

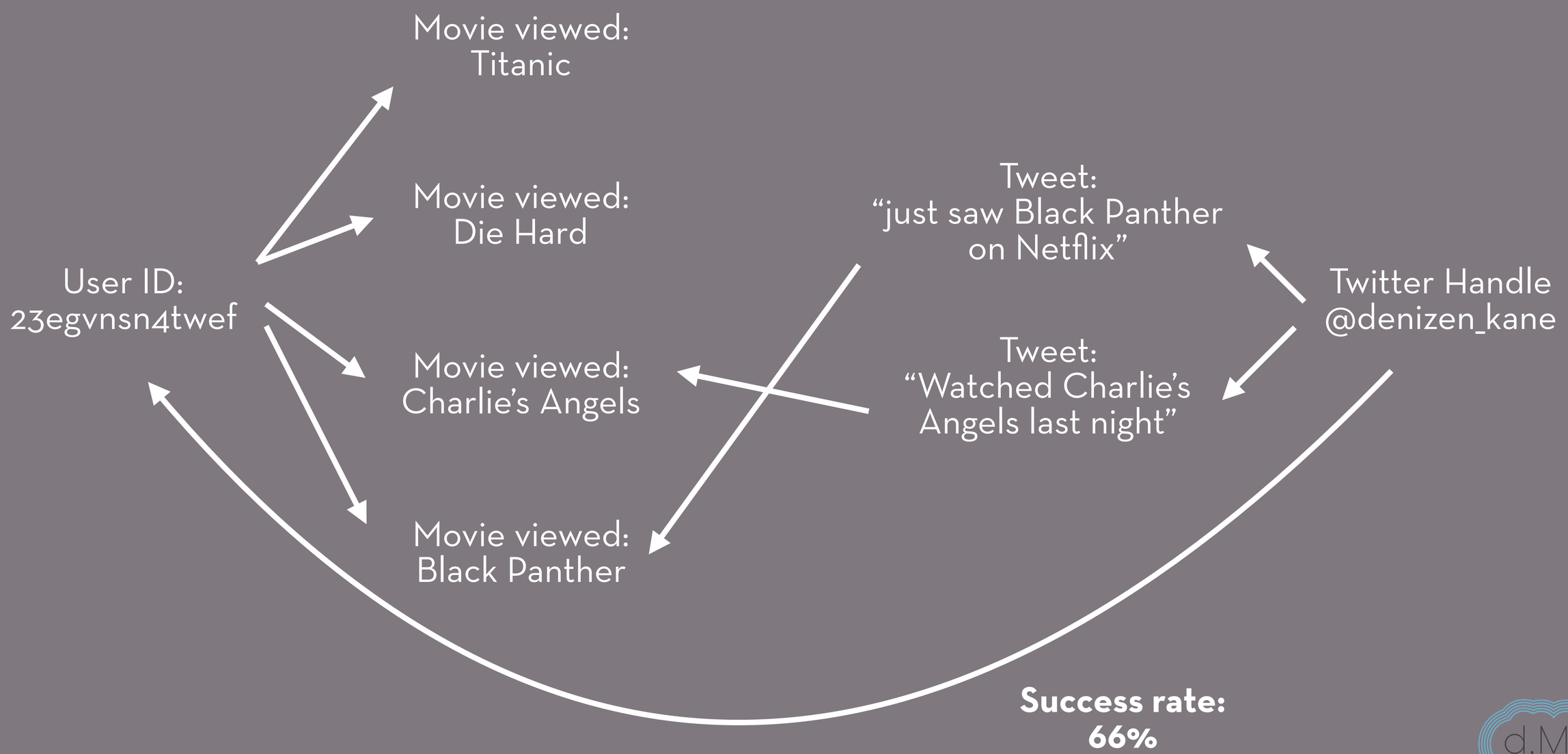
Our contributions. Our first contribution is a formal model for privacy breaches in anonymized micro-data

User ID:
23egvnsn4twef


User ID:
23egvnsn4twef
Movie viewed:
Titanic
Movie viewed:
Die Hard
Movie viewed:
Charlie's Angels
Movie viewed:
Black Panther


User ID:
23egvnsn4twef
Movie viewed:
Titanic
Movie viewed:
Die Hard
Movie viewed:
Charlie's Angels
Movie viewed:
Black Panther
Tweet:
"just saw Black Panther
on Netflix"
Tweet:
"Watched Charlie's
Angels last night"
Twitter Handle
@denizen_kane


Movie viewed:
Titanic
Movie viewed:
Die Hard
User ID:
23egvnsn4twef
Movie viewed:
Charlie's Angels
Movie viewed:
Black Panther
Tweet:
"just saw Black Panther
on Netflix"
Tweet:
"Watched Charlie's
Angels last night"
Twitter Handle
@denizen_kane


Movie viewed:
Titanic
Movie viewed:
Die Hard
User ID:
23egvnsn4twef
Movie viewed:
Charlie's Angels
Movie viewed:
Black Panther
Tweet:
"just saw Black Panther
on Netflix"
Tweet:
"Watched Charlie's
Angels last night"
Twitter Handle
@denizen_kane
Success rate:
66%


Movie viewed:
Titanic
Movie viewed:
Die Hard
User ID:
23egvnsn4twef
Movie viewed:
Charlie's Angels
Movie viewed:
Black Panther
Tweet:
"just saw Black Panther
on Netflix"
Twitter Handle
@denizen_kane
Tweet:
"Watched Charlie's
Angels last night"
Tweet:
"Donald Trump Sucks"

d.ML

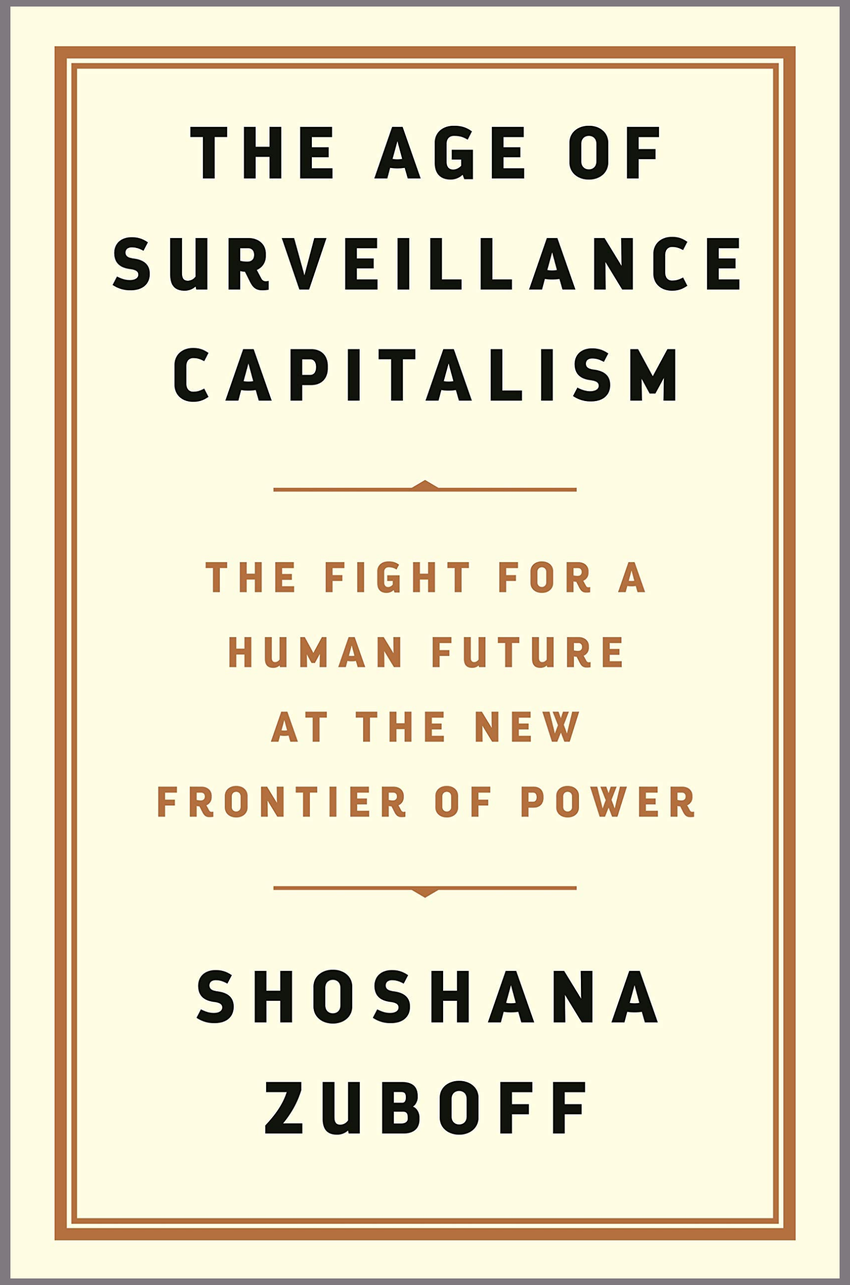
The de-anonymization was robust to:

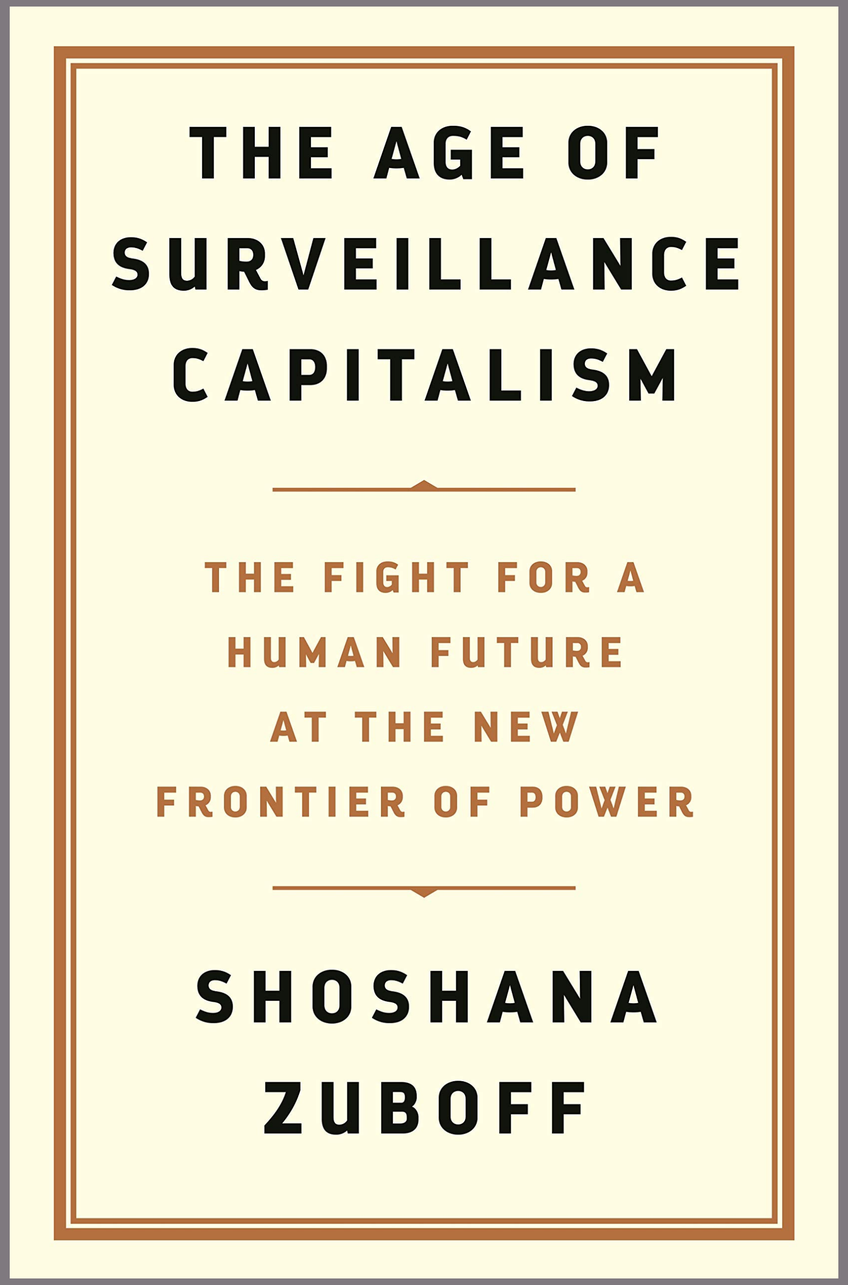
- Erroneous/imprecise ratings
- Missing data points
- Long time windows
- Inclusion of incorrect data (fake users/movies)
- Anonymized movie titles (no meta-data)

When you collect data at scale, you implicitly know more about your users than you bargained for

When you collect data at scale, you implicitly know more about your users than you bargained for

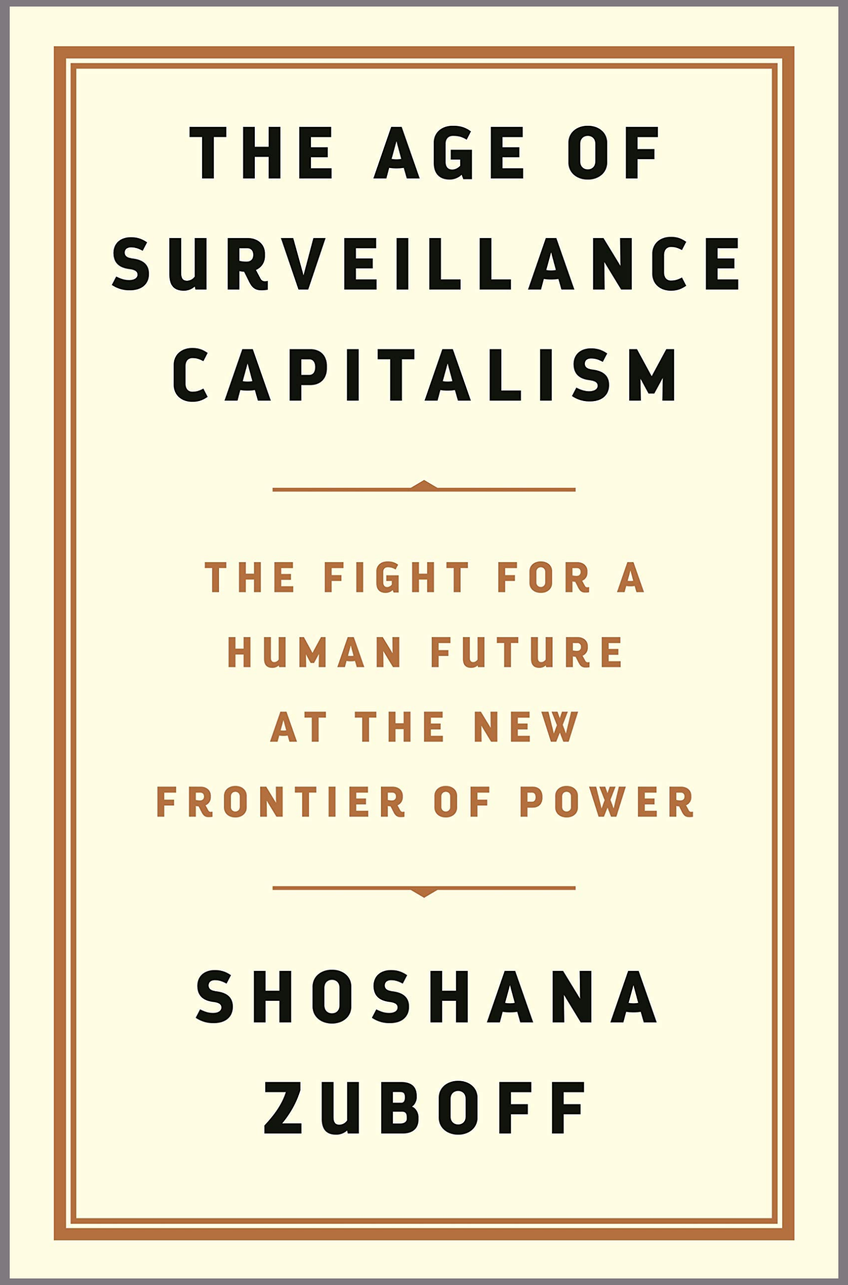
Sexual Orientation, Political Preference, Mental Health, Drug Use, Religious Affiliation, etc.


THE AGE OF SURVEILLANCE CAPITALISM
THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER
SHOSHANA ZUBOFF



"...behavioral prediction markets..."

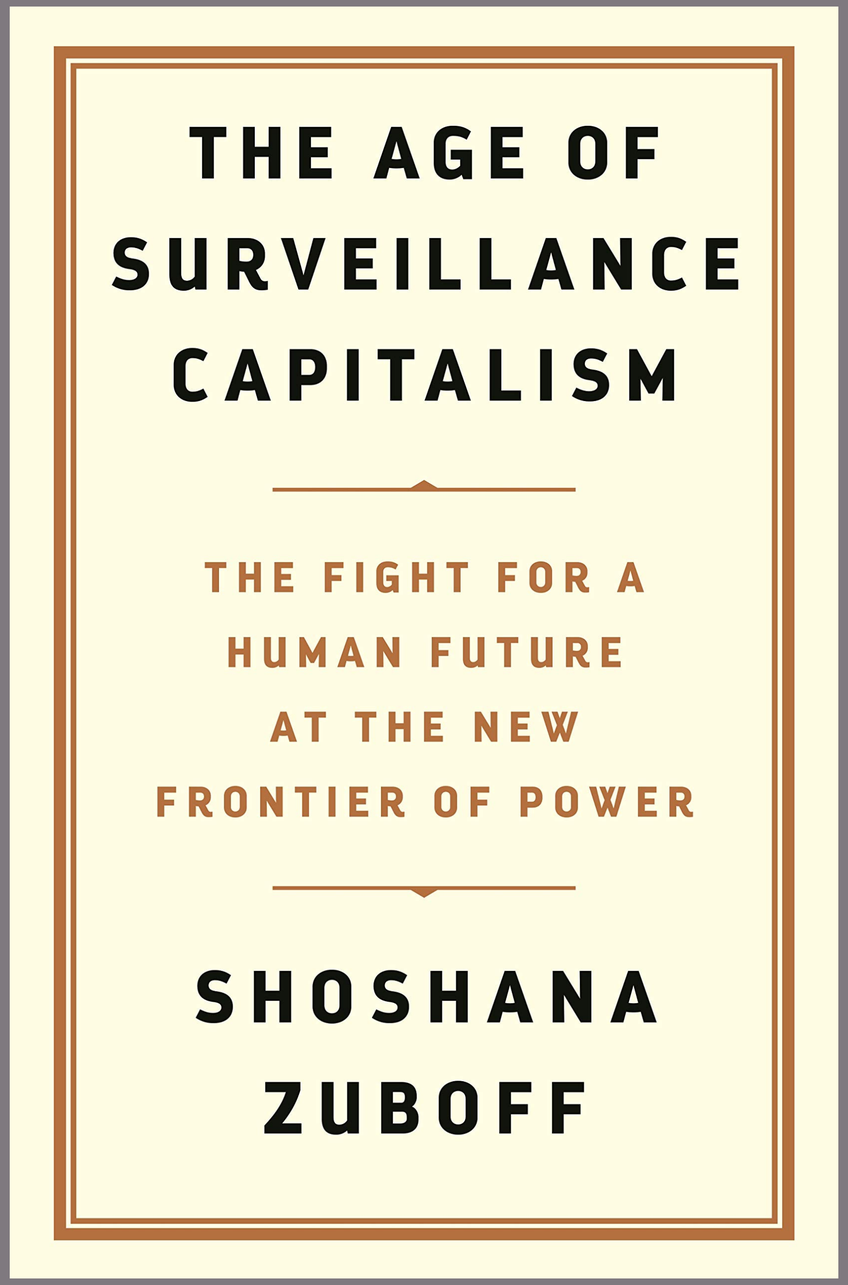
d.ML



"...behavioral prediction markets..."

- Personalized advertising
- Re-targeting
- Insurance pricing
- Persuasive messaging
- Sponsored gamification
- Political advertisements

d.ML



"...freedom to the future tense..."

d.ML

THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER

SHOSHANA ZUBOFF

"...freedom to the future tense..."

d.ML

THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER

SHOSHANA ZUBOFF

"...freedom to the future tense..."

Activision wins patent that uses matchmaking to make you want to buy stuff

By James Davenport October 17, 2017

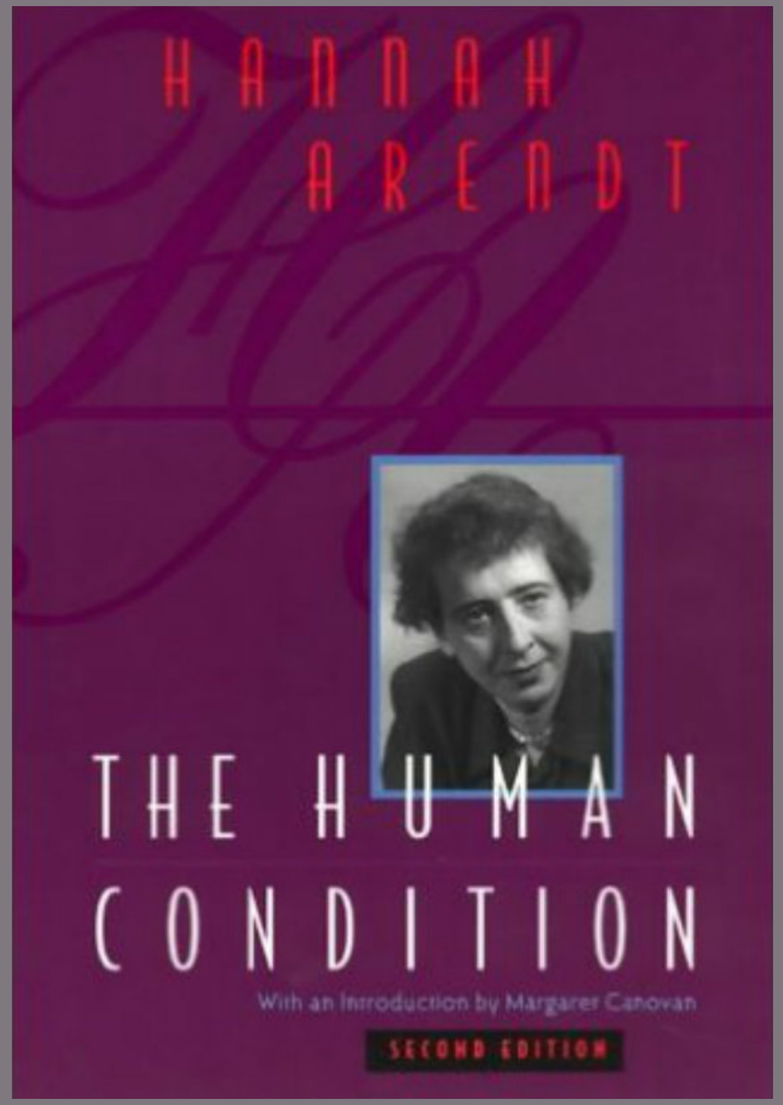
Activision says the system is not is in place.

COMMENTS

d.ML

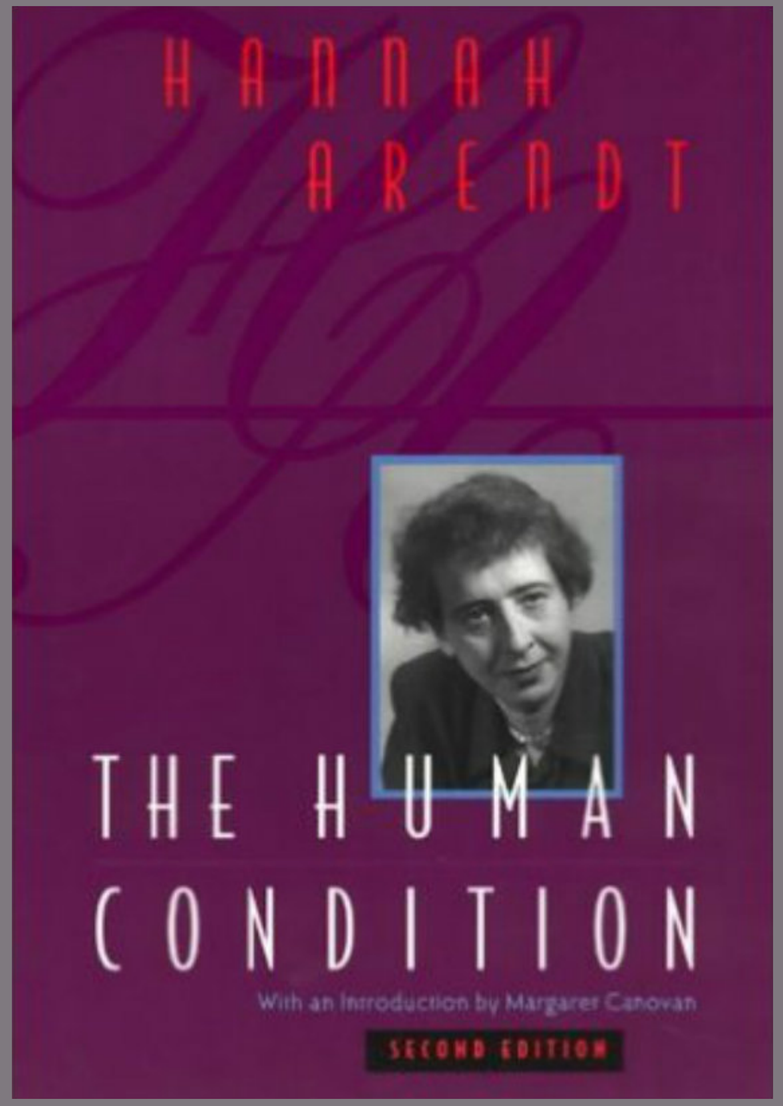
Is this simply a “privacy issue”?

*"For us, appearance—**something that is being seen and heard by others** as well as by ourselves—constitutes reality."*



*"For us, appearance—**something that is being seen and heard by others** as well as by ourselves—constitutes reality."*

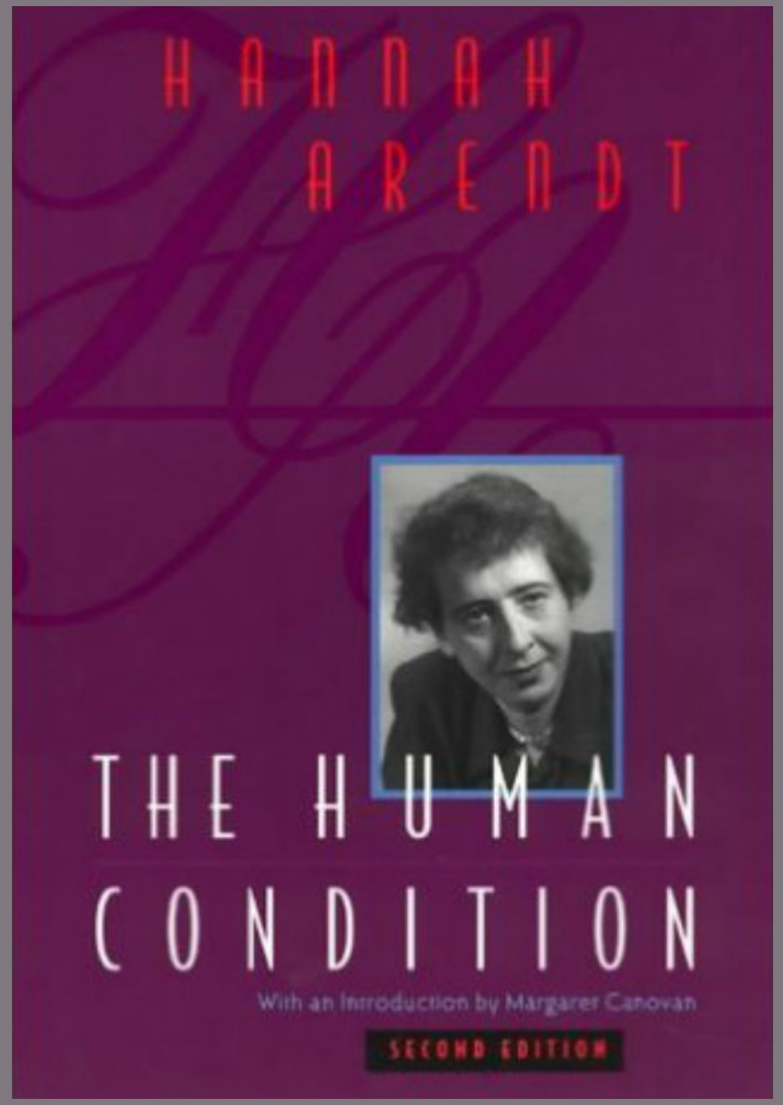
*"Yet there are a great many things which cannot withstand the **implacable, bright light of the constant presence of others** on the public scene"*



d.ML

"Yet there are a great many things which cannot withstand the ***implacable, bright light of the constant presence of others*** *on the public scene"*

Power is "a potential and not an unchangeable, measurable and reliable entity like force or strength ... [it] ***springs up between men when they act together and vanishes the moment they disperse****"*



Is this simply a “privacy issue”?