A critical review of 10 years of Privacy Technology

Seda Gürses
Sniff, Scrape, Crawl...
Piet Zwart Institute
Rotterdam, The Netherlands

WHAT?

- ★ REVIEW PRIVACY TECHNOLOGIES
  - ◉ REFLECTING ON RESEARCH
  - ◉ START A ROBUST DISCUSSION
    - ✳ SUCCESSES AND FAILURES
- ✤ ASSUMPTIONS
- ✤ ASPIRATIONS
- ✤ LIMITATIONS
- ✤ FUTURE STEPS

privacy

data protection

privacy

non-absolute

contextual

relational

opacity of the individual

data protection

privacy

non-absolute

contextual

relational

opacity of the individual

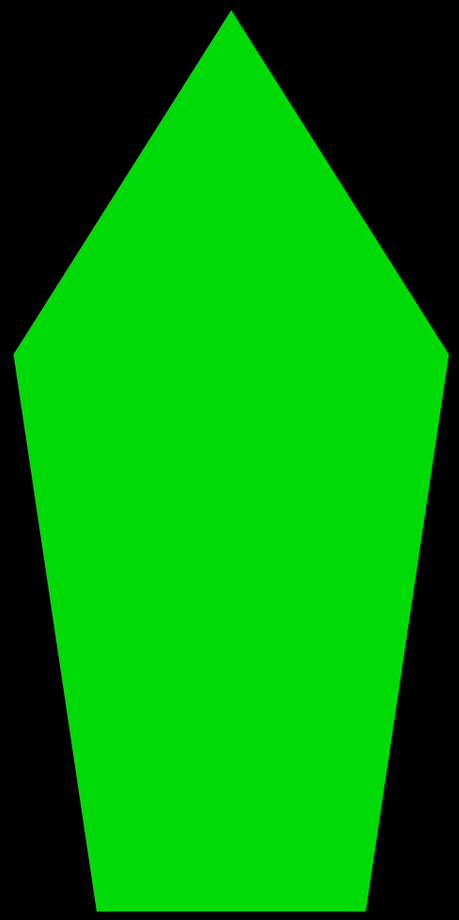
data protection

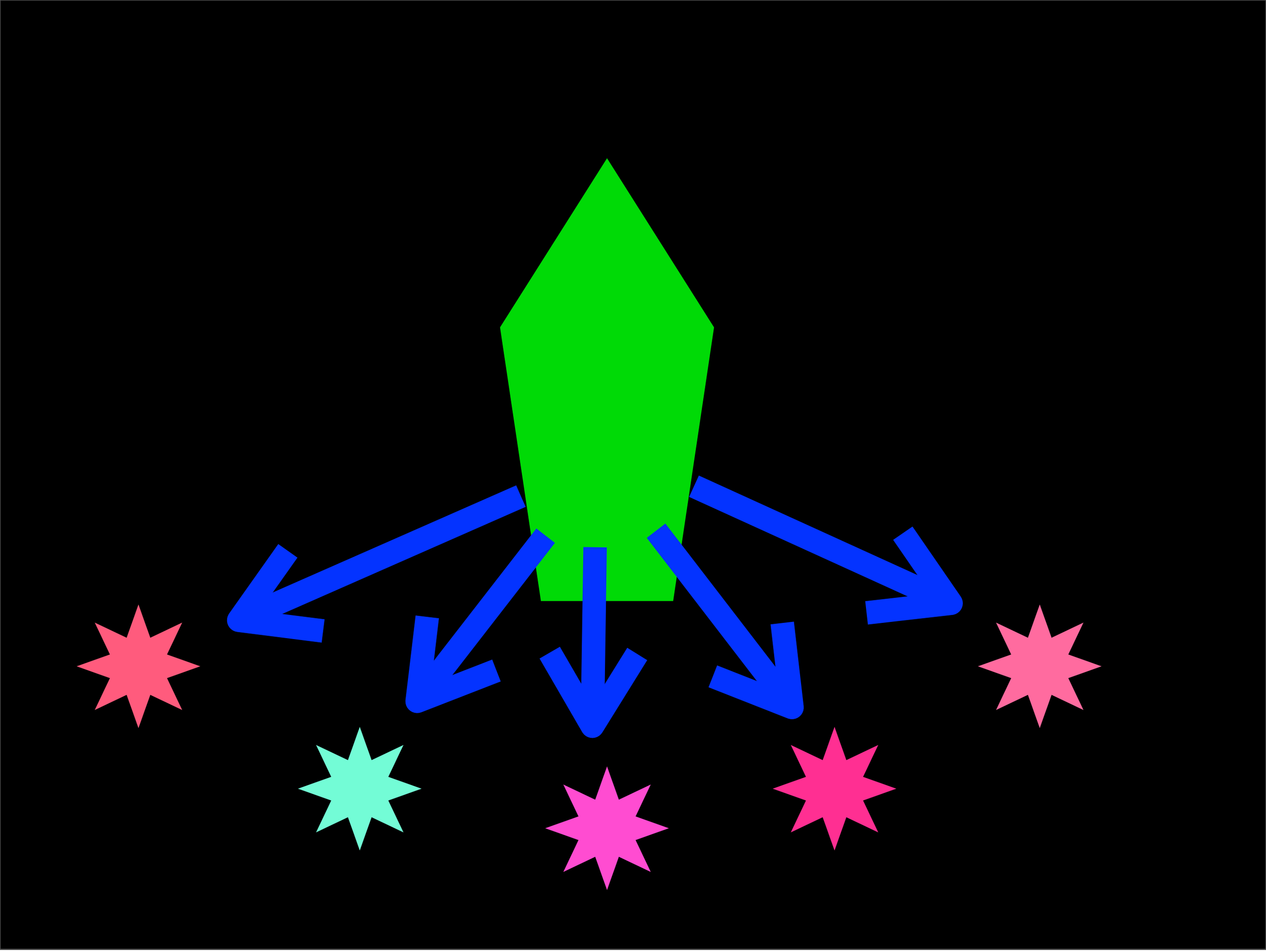
procedural safeguards

accountability

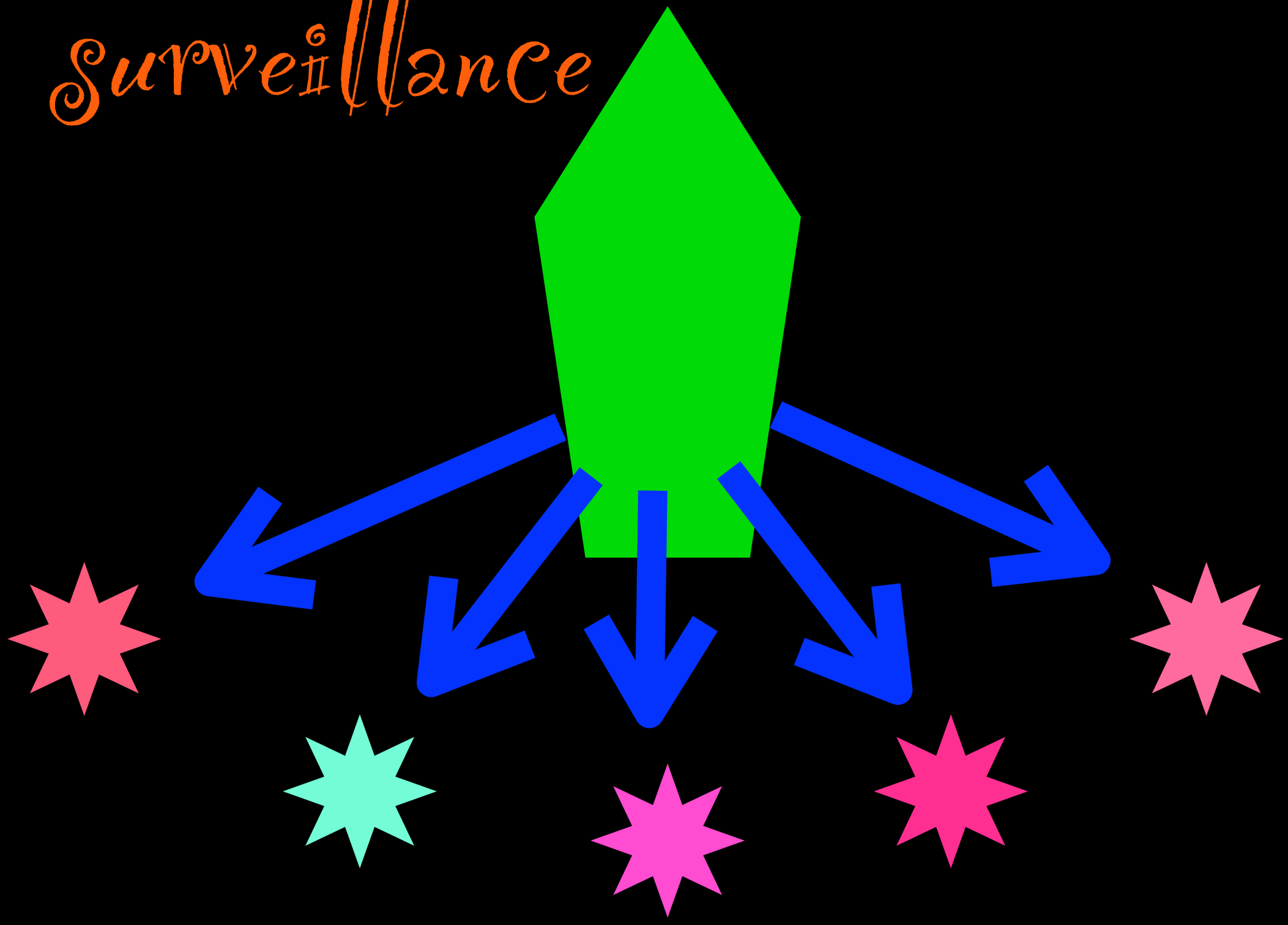
transparency

personal data





Surveillance



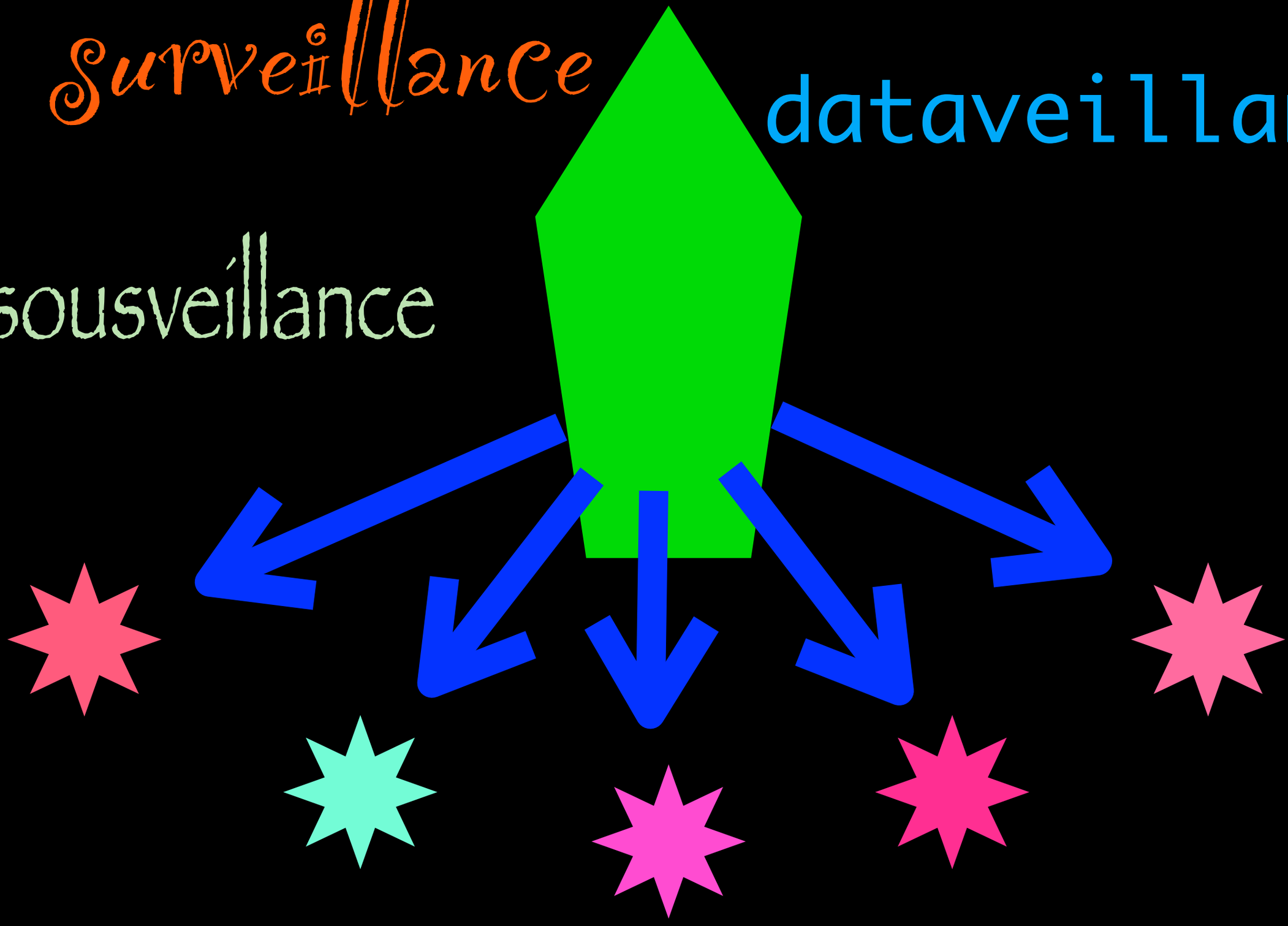
Surveillance

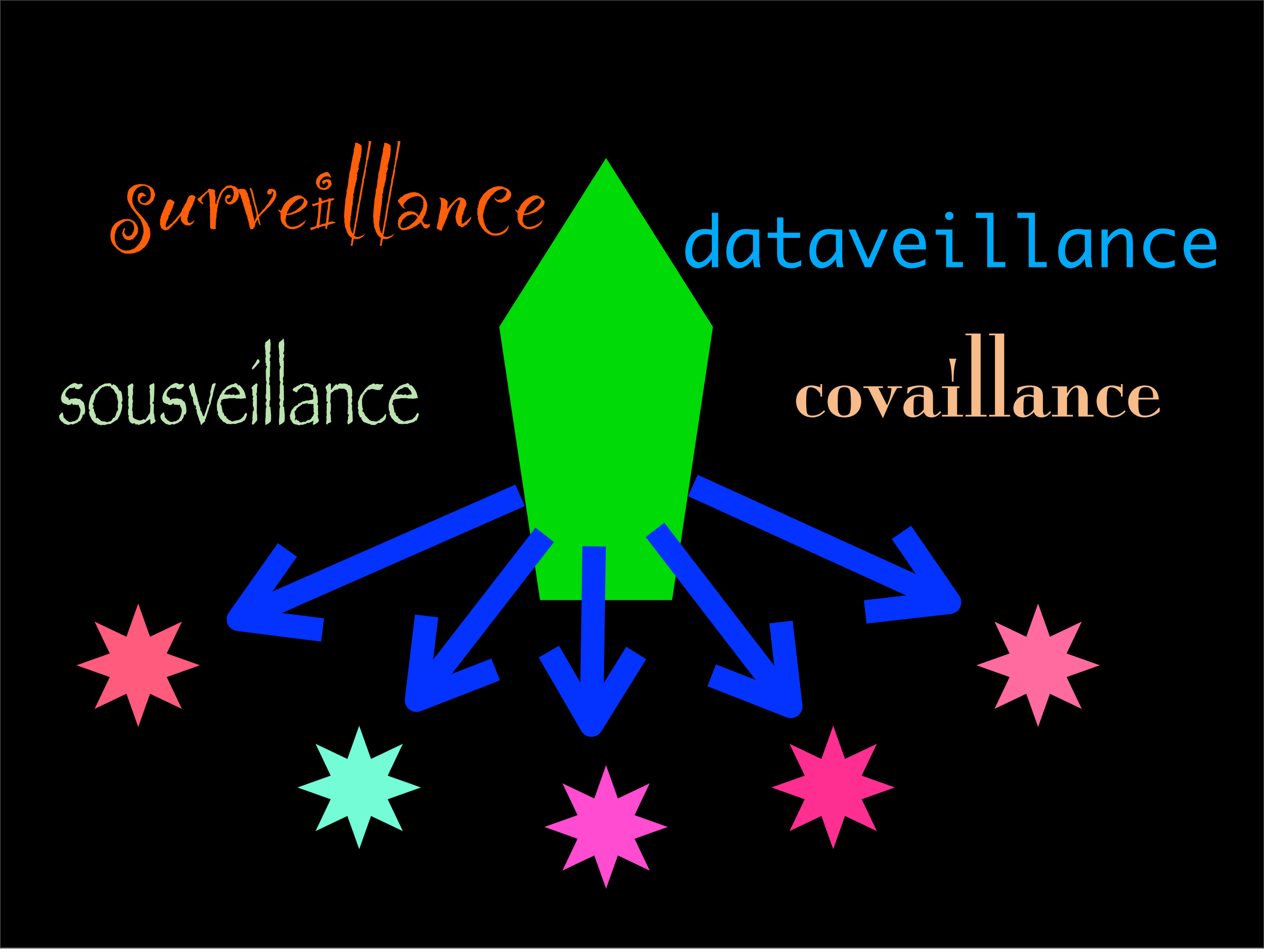
sousveillance

Surveillance

dataveillance

sousveillance




Surveillance
dataveillance
sousveillance
covaillance

PRIVACY RESEARCH PARADIGMS

hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

PRIVACY RESEARCH PARADIGMS

hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy
as control

separation of identities, data protection principles

PRIVACY RESEARCH PARADIGMS

hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy
as control

separation of identities, data protection principles

privacy
as practice

the freedom from unreasonable constraints on the construction of one's own identity (Agre, 1999)

transparency and feedback

PRIVACY RESEARCH PARADIGMS

hiding information and identity

privacy as confidentialit

privacy as control

separation of identities, data protection principles

privacy as practice

transparency and feedback

privacy
as confidentiality

SHORT HISTORY

- 69 FIRST DISCUSSIONS
  - CONCERNS ABOUT CENTRALIZED DATABASES
  - CONFIDENTIALITY BETWEEN USERS/ADMINS
- 80s
  - CHAUM'S PROPOSAL FOR ANON-COMMUNICATIONS
    - CONFIDENTIALITY OF
    - CONTENT + WHO IS COMMUNICATING
    - ANDREAS PFITZMANN, BRIGIT PFITZMANN, MICHAEL WAIDNER
  - CHAUM'S PROPOSAL FOR BLIND SIGNATURES
    - AUTHENTICITY + ANONYMITY

SHORT HISTORY

- ★ 90s
  - ✤ Chaum develops a scheme for anon-cash
  - ✤ Brands' scheme for single show selective disclosure credentials
  - ✤ Camenisch multiple-show selective disclosure credentials
  - ✤ main idea:
    - ◉ minimize data revealed during authentication / authorization
    - ◉ zero-knowledge proofs

SHORT HISTORY

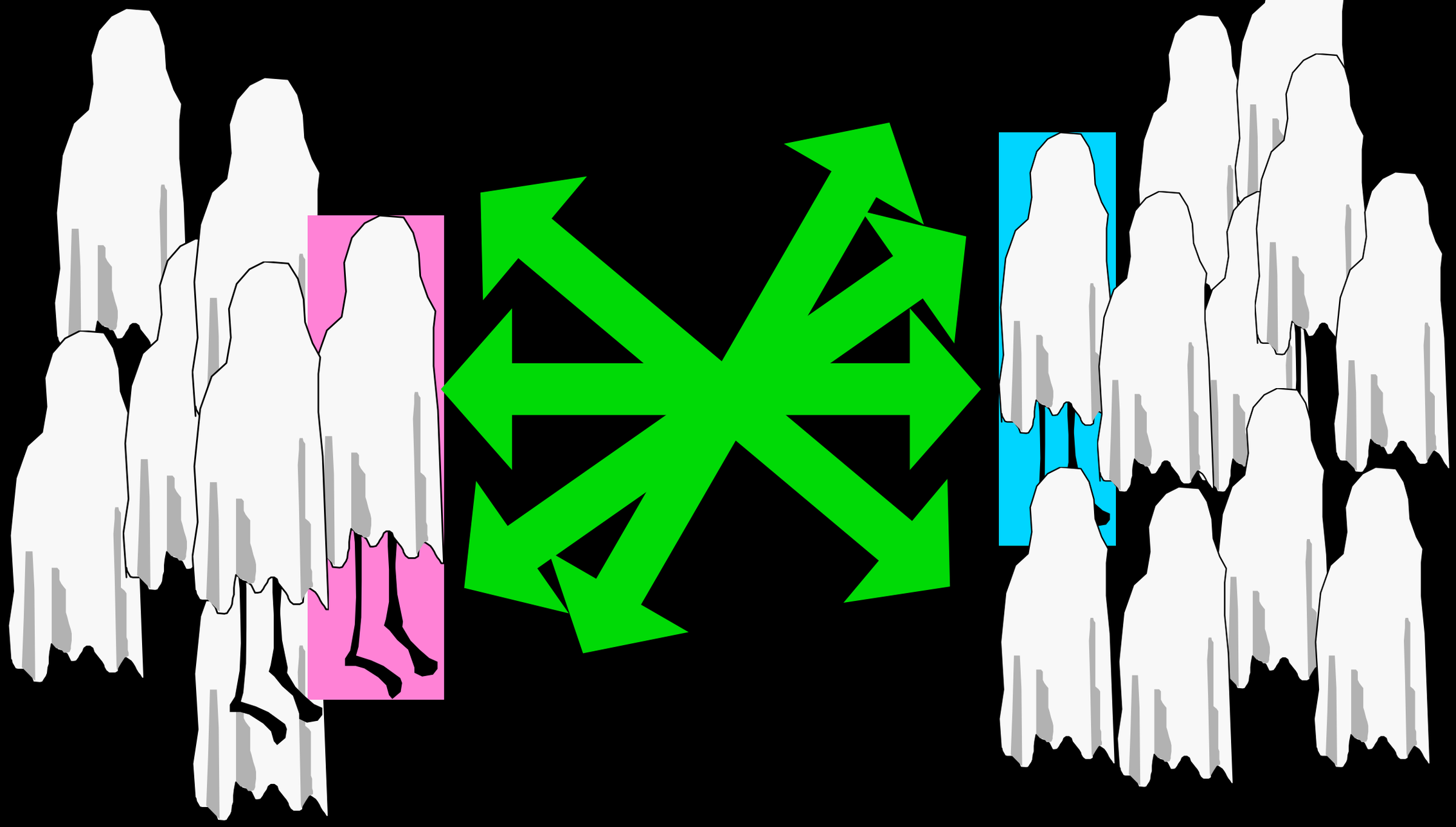
★ 00s

✣ EXTENSION OF THE COMMUNITIES

- Privacy Enhancing Technologies Symposium (PETs)
- Workshop on Privacy in the Electronic Society
- Workshop on the Economics of Information Security
- Symposium on Security and Privacy

ANONYMIZERS

THE CONCEPT



ANONYMIZERS

THE MODEL

- OBSERVER (ADVERSARY)
  - DOES NOT KNOW WHO IS COMMUNICATING WITH WHOM
    - PROBABILISTIC MODELS
- VARYING DEGREES OF ANONYMITY:
  - ENTROPY BASED METRICS
    - THE THRESHOLD PROBLEM
- USERS TRACES DELINKED FROM IDENTITY

DB ANONYMIZATION

- ★ PPDP - PPDM
- ★ BASIC IDEA:
  - ✤ HIDE THE INDIVIDUALS IN THE DB
  - ✤ KEEP THE UTILITY OF THE DATA
  - ✤ ECONOMIC / DP APPROACH
- ★ CONCEPT OF K-ANONYMITY

Name	Date of Birth	Gender	Zip Code	Disease
Neset	22/03/1983	Male	10974	Flu
Süleyman	03/03/1984	Male	10943	Diabetes
Caroline	15/06/1973	Female	12078	Flu
Erika	30/02/1975	Female	12078	AIDS
Thomas	28/11/1990	Male	12546	AIDS
Thibaut	13/08/1996	Male	12503	Flu
Özge	29/10/1980	Female	10030	Arthritis
Fahriye	02/04/1984	Female	10030	Diabetes

privacy
as confidentiality?

ANONYMIZATION FAIL!

- ★ SHMATIKOV AND NARAYANAN SHOW THAT:
  - ✤ YOU CAN ALWAYS LINK DISPARATE INFORMATION SOURCES AND IDENTIFY INDIVIDUALS
  - ✤ SO, WHAT'S WITH PERSONAL DATA?
- ★ TRY DIFFERENTIAL PRIVACY...
  - ✤ VERY THEORETICAL INTERACTIVE PRIVACY PRESERVING QUERYING SYSTEM

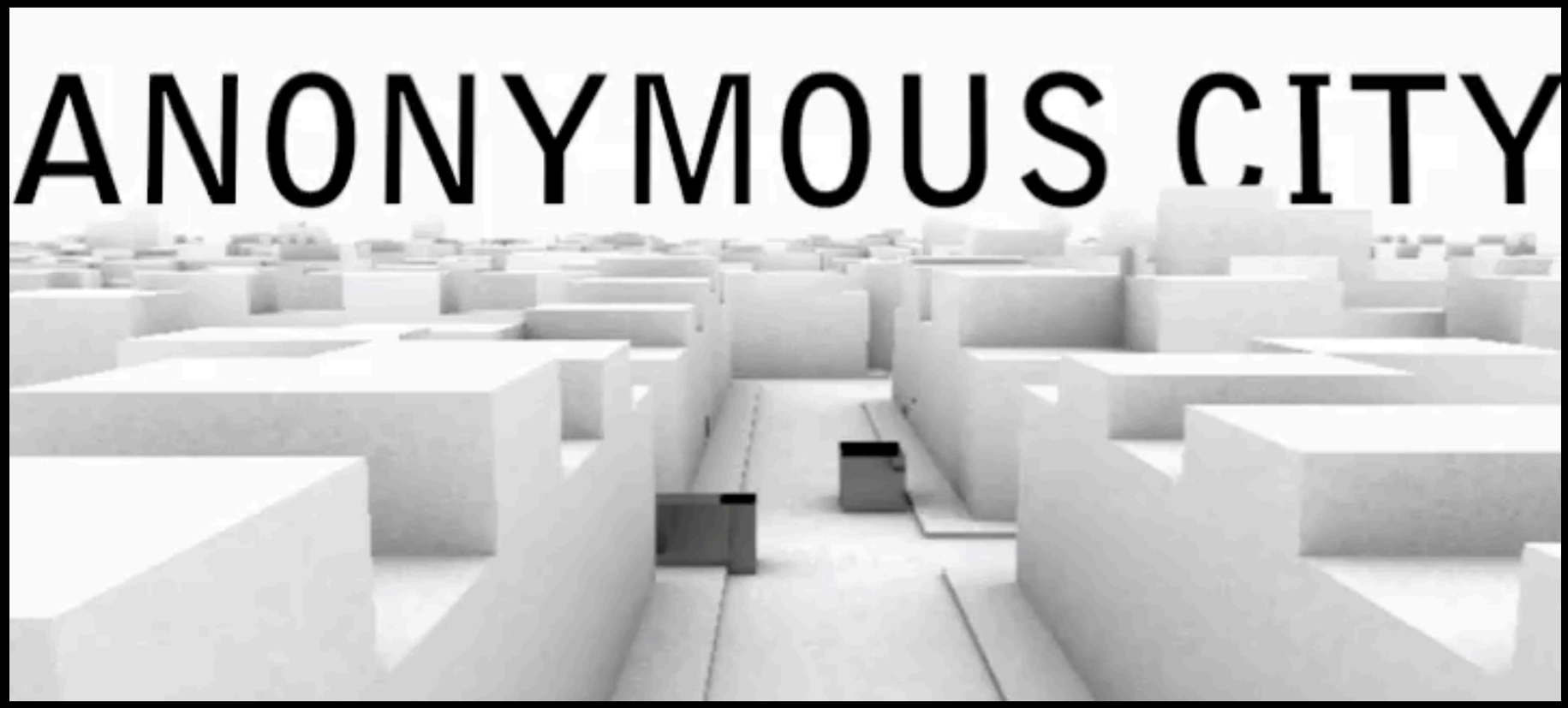
ANONYMIZATION

- AN ECONOMIC LOGIC
  - SURVEILLANCE IS INTACT
- DATA PROTECTION AT UNEASE
  - PERSONAL DATA?
- FURTHER RESEARCH ON IMPACT AND STRATEGIES NEEDED

ANONYMIZERS

THE ASSUMPTIONS

1. THERE IS NO TRUST ON THE INTERNET
2. USERS ARE INDIVIDUALLY RESPONSIBLE FOR MINIMIZING THE COLLECTION AND DISSEMINATION OF THEIR DATA
3. IF THEY KNOW YOUR DATA THEN THEY KNOW YOU
4. COLLECTION AND PROCESSING OF PERSONAL DATA, IF USED AGAINST YOU, WILL HAVE A CHILLING EFFECT
5. TECHNICAL SOLUTIONS SHOULD BE PREFERRED INSTEAD OF RELYING ON LEGAL SOLUTIONS



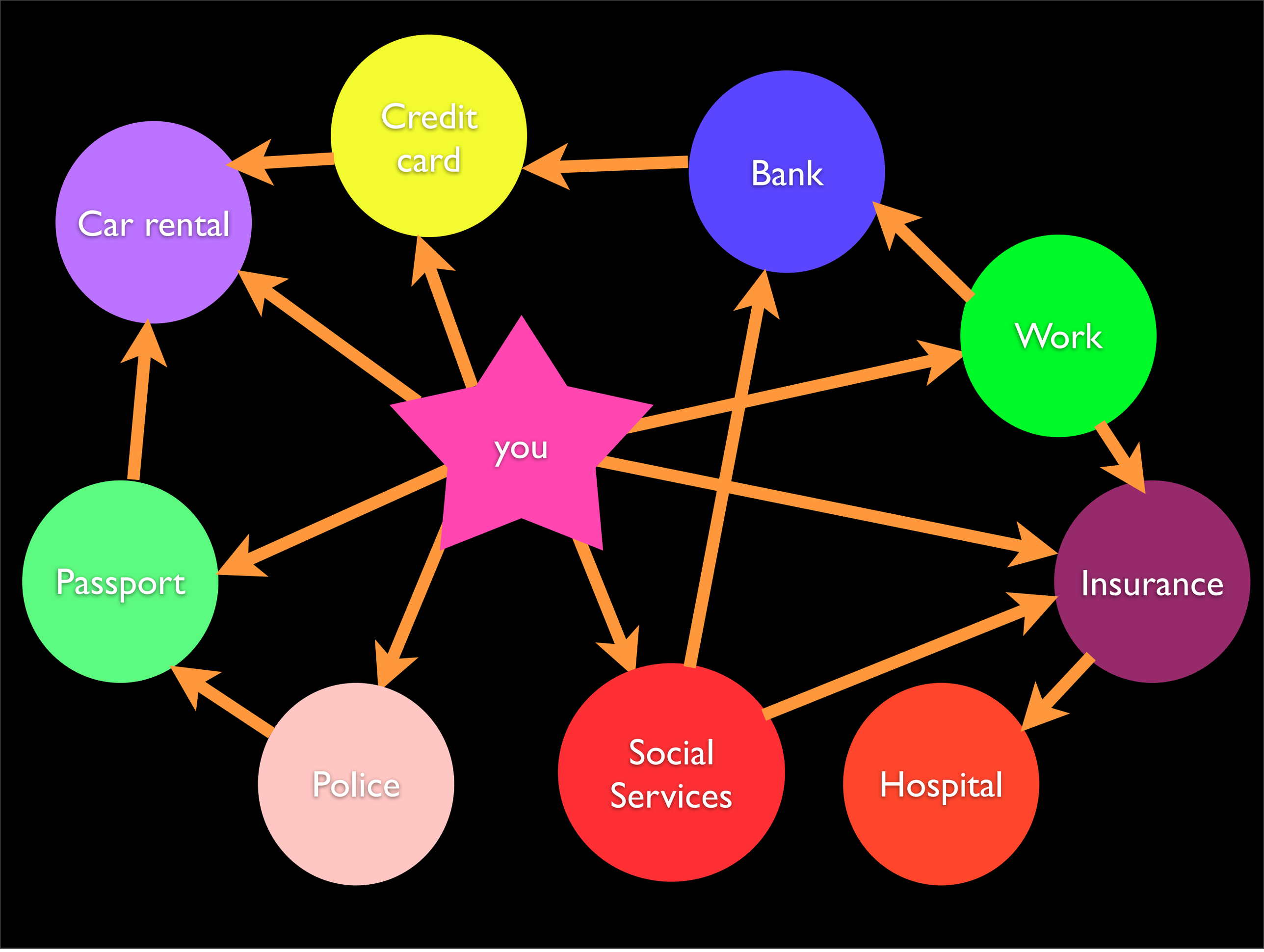
ANONYMOUS CITY:

A SHORT FILM THAT SHOWS A CITY IN WHICH ABSOLUTE ANONYMITY IS ATTAINED. THE FILM DEPICTS BOTH HOW SUCH A STATE OF AFFAIRS WOULD REQUIRE ALL INDIVIDUALS TO HYPER-CONTROL THEIR ACTIVITIES IN ORDER TO HAVE "PRIVACY". IT ALSO MAKES EVIDENT THE SECURITY RESEARCH CHALLENGES INHERENT TO MAKING SUCH SYSTEMS, AS THEY ARE USED TODAY AS STRATEGIC COUNTER-SURVEILLANCE TOOLS, ROBUST AGAINST ADVERSARIES.

ANONYMIZERS
ASSUMPTIONS

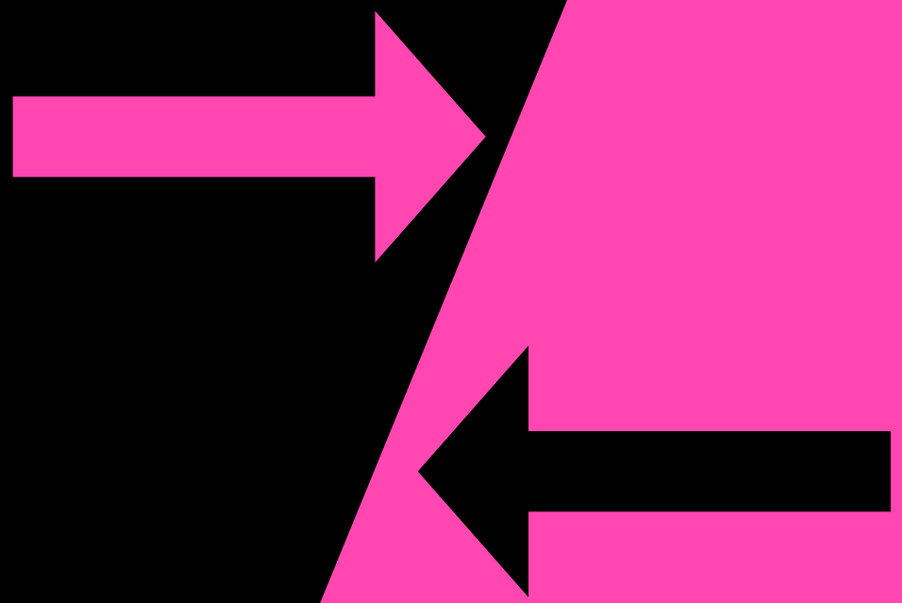
1. THERE IS NO TRUST ON THE INTERNET
2. USERS ARE INDIVIDUALLY RESPONSIBLE FOR MINIMIZING THE COLLECTION AND DISSEMINATION OF THEIR DATA
3. IF THEY KNOW YOUR DATA THEN THEY KNOW YOU
4. COLLECTION AND PROCESSING OF PERSONAL DATA, IF USED AGAINST YOU, WILL HAVE A CHILLING EFFECT
5. TECHNICAL SOLUTIONS SHOULD BE PREFERRED INSTEAD OF RELYING ON LEGAL SOLUTIONS


you

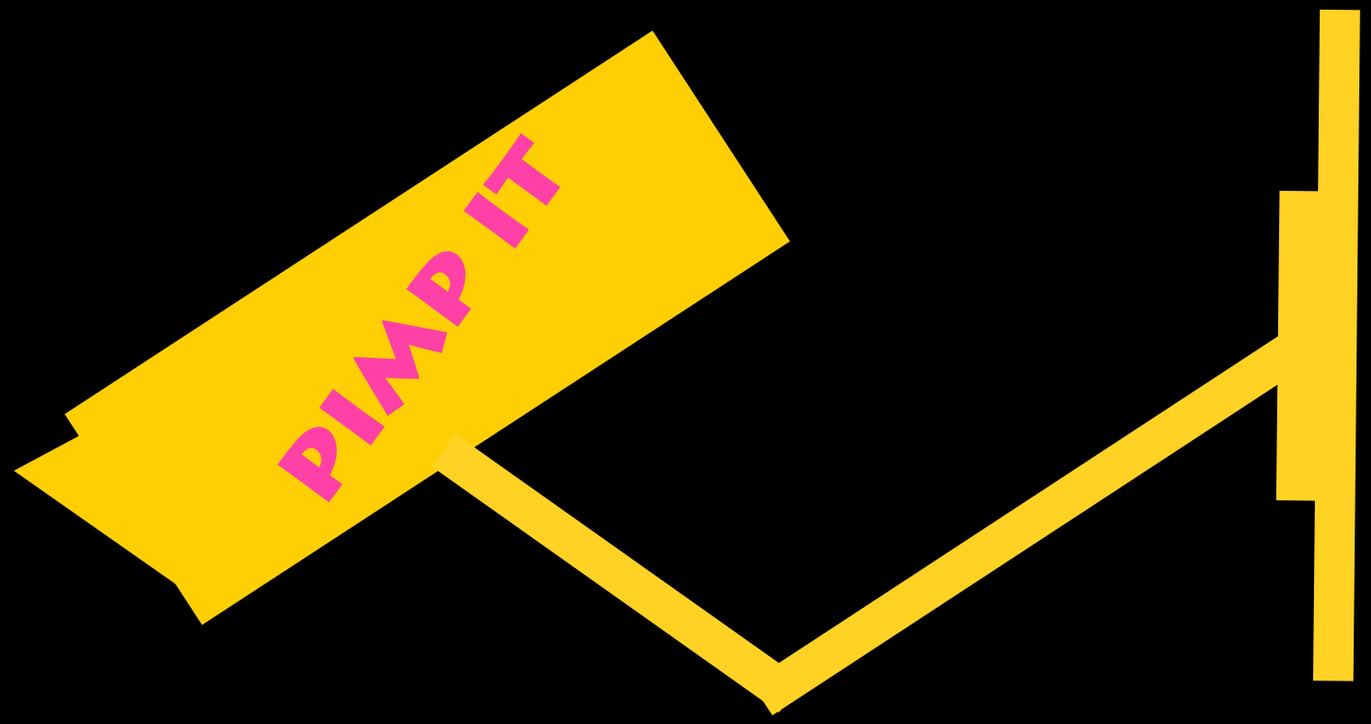

Credit card
Car rental
Bank
Work
you
Passport
Insurance
Police
Social Services
Hospital

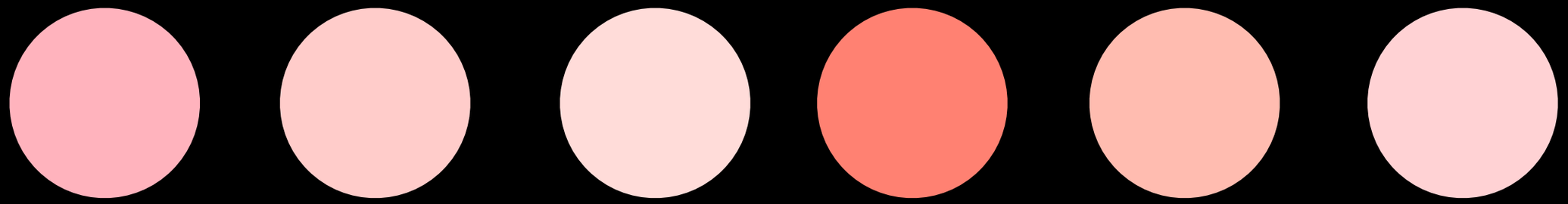

categories
UNDESIRABLE
database
database
royalty
MARKETING
geodemographic systems
dead weight loss
market
categories
database
customer
market
DISCOURSE
TING
database
royalty
customer
CRM
market
database
customer
market
customer
dead weight loss
royalty
CRM

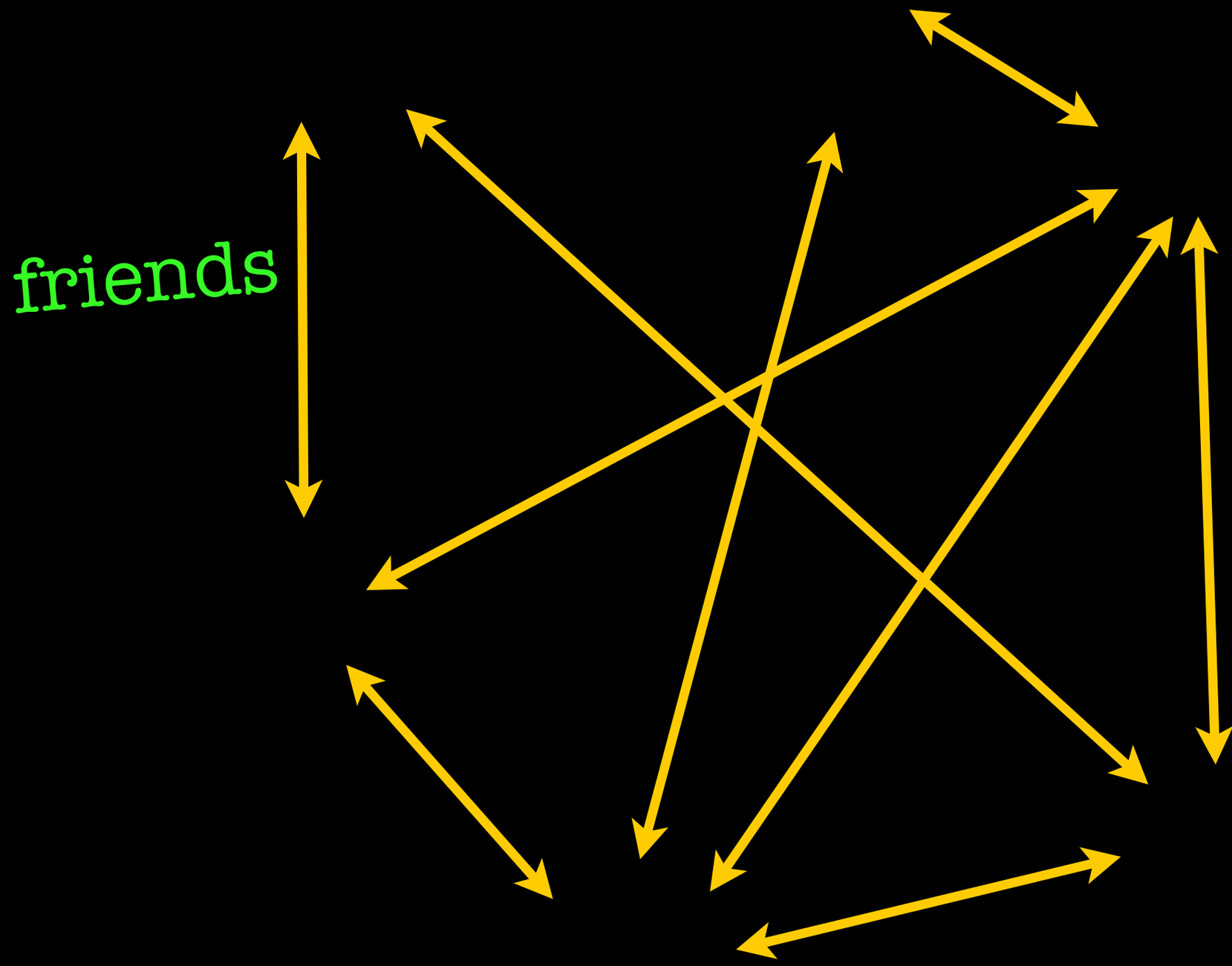
private

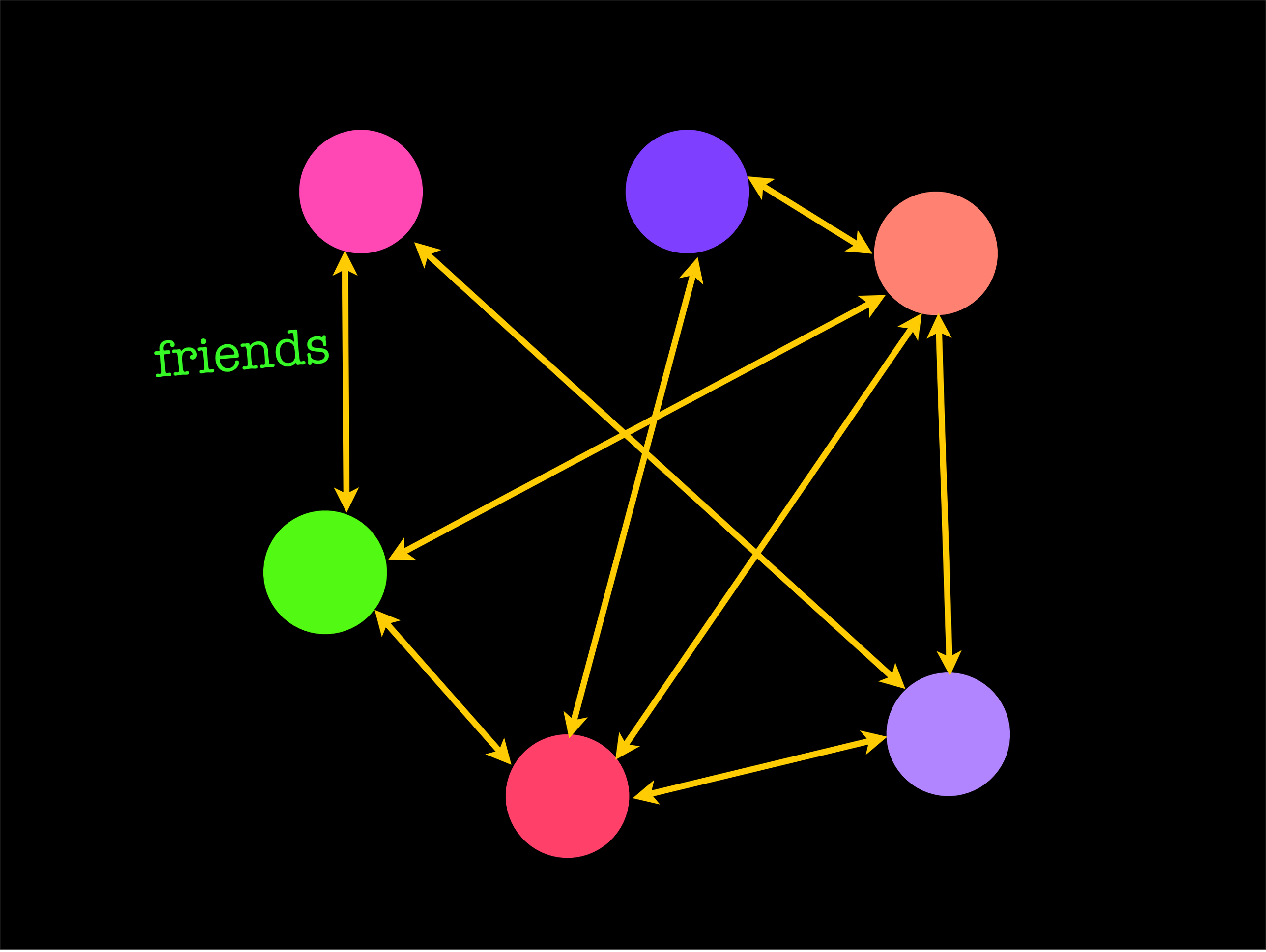


public

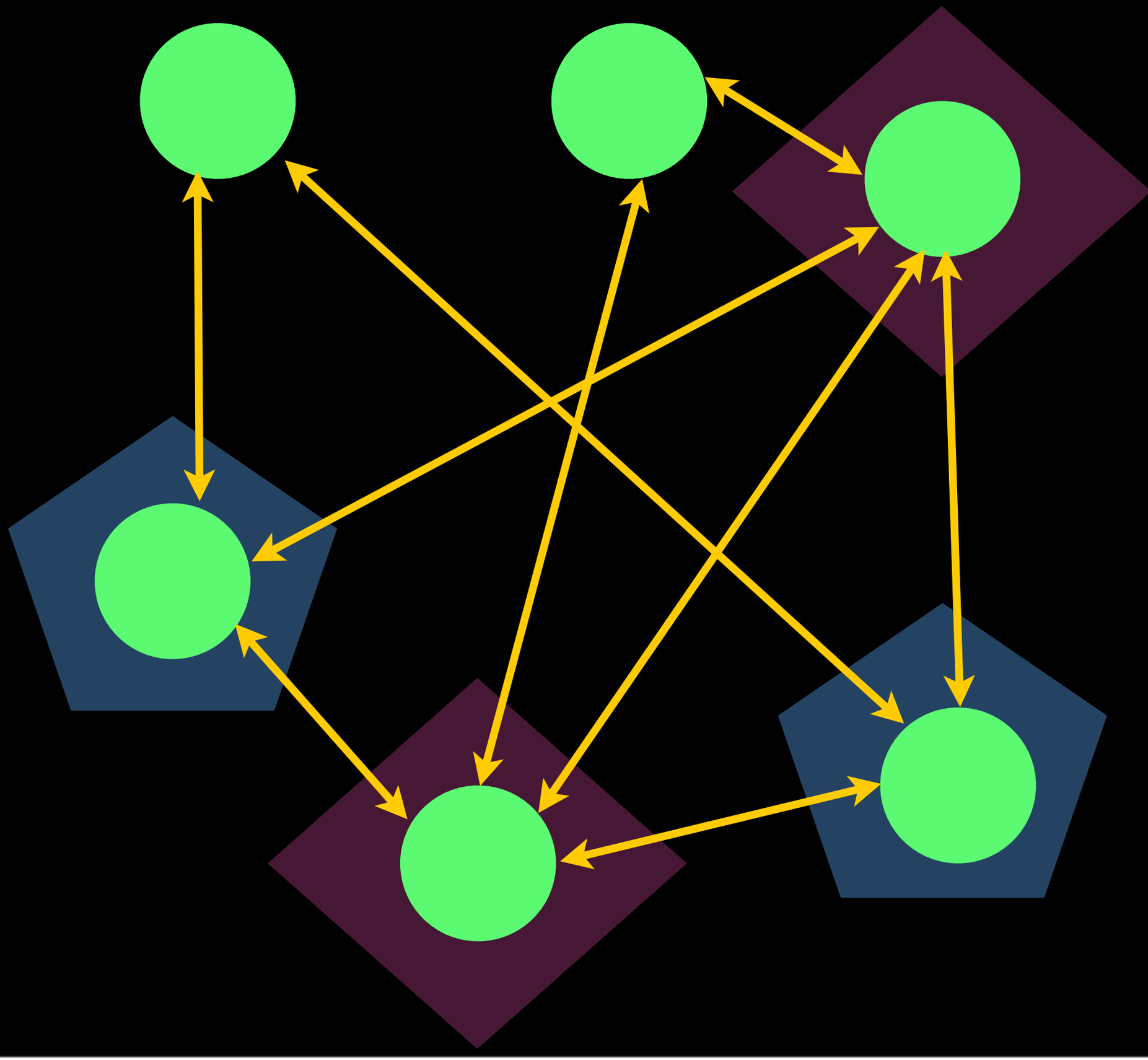

PIMP IT

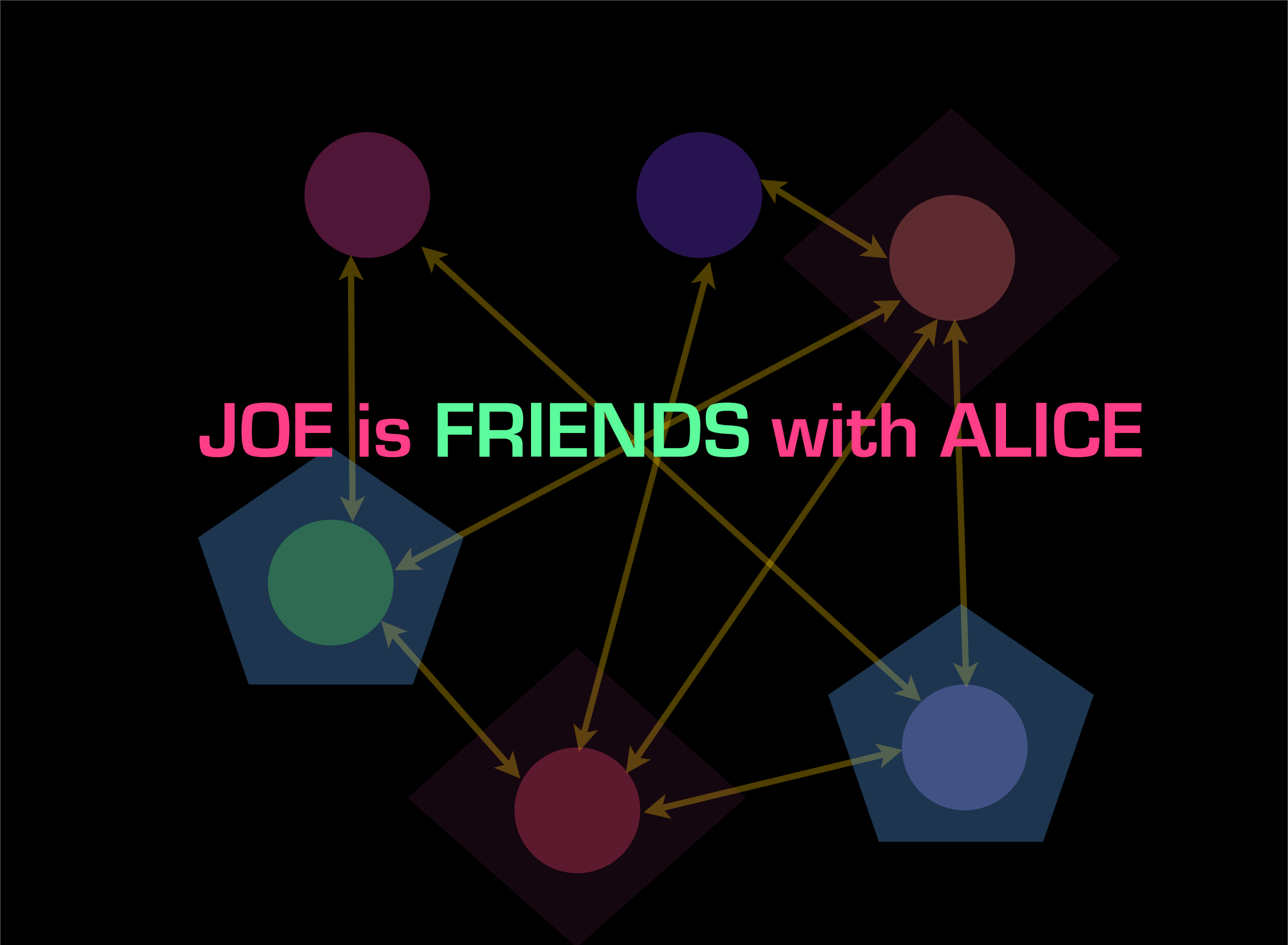



friends


friends

joe has 3 friends, alice has 4 friends




JOE is FRIENDS with ALICE

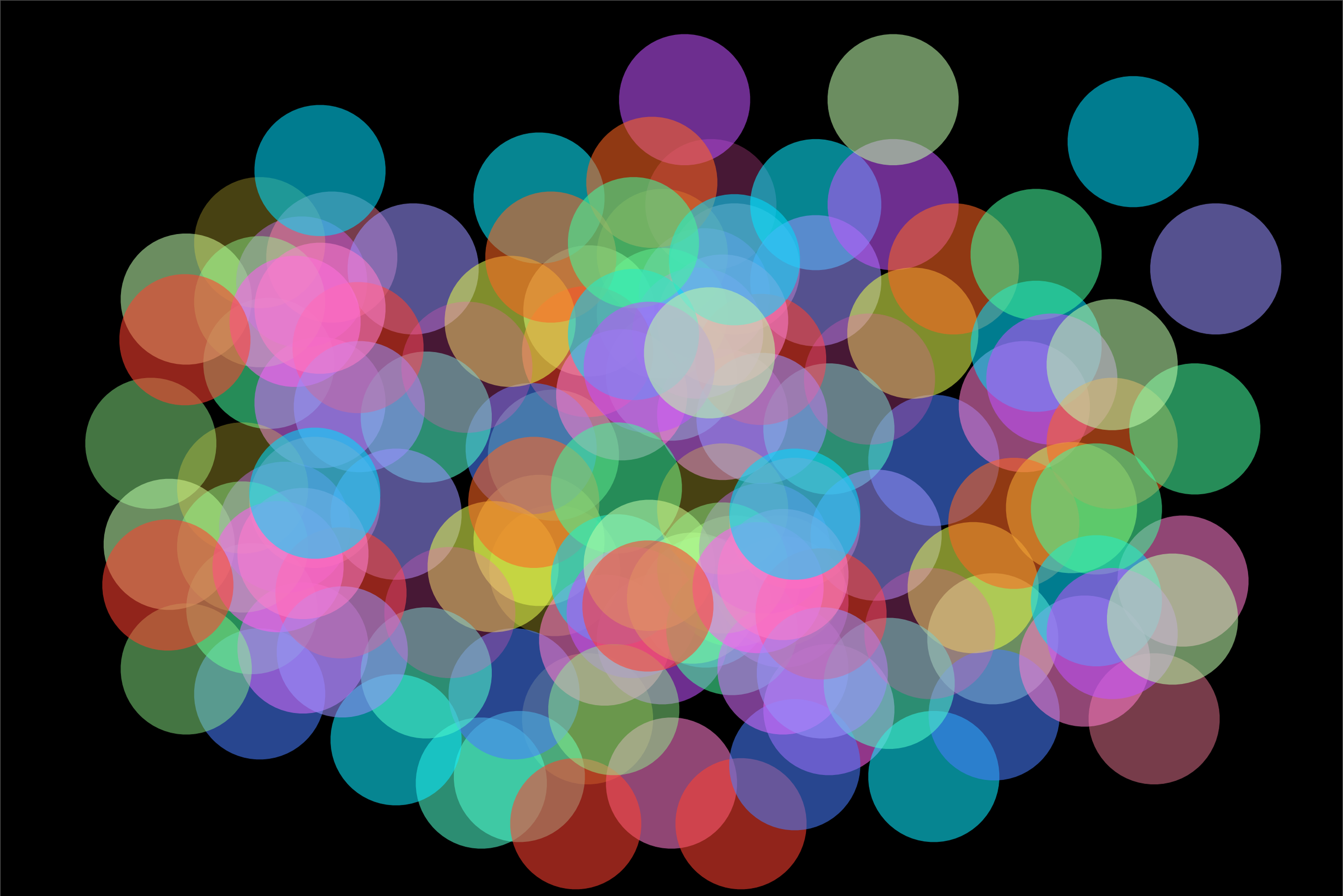
ANONYMOUS
IS
VOGELFREI

ANONYMOUS

X

PERSISTENCE

PRIVATE INDIVIDUALS


COLLECTIVES


DETACHMENT

STRATEGIC REVELATION

privacy
as control

SHORT HISTORY

- IDENTITY MANAGEMENT SYSTEMS
  - 90s
    - MICROSOFT PASSPORT
      - SINGLE-SIGN ON
      - SHUNNED: LOCKING CUSTOMERS
  - LIBERTY ALLIANCE (OASIS)
    - FEDERATED IDENTITY MANAGEMENT

SSO

identity provider

relying party

user

SSO

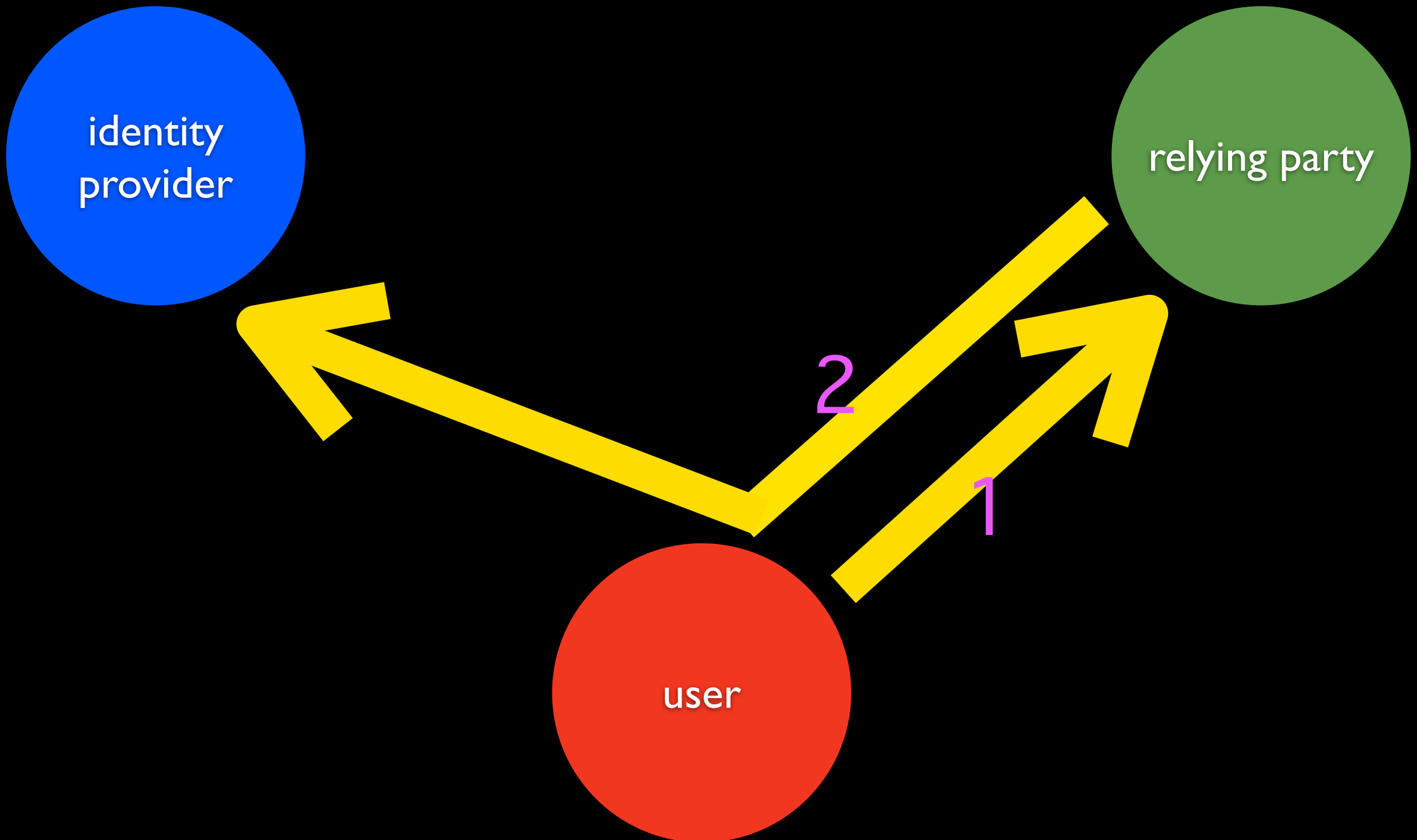
identity provider

relying party

user

1

SSO



SSO

identity provider

relying party

2

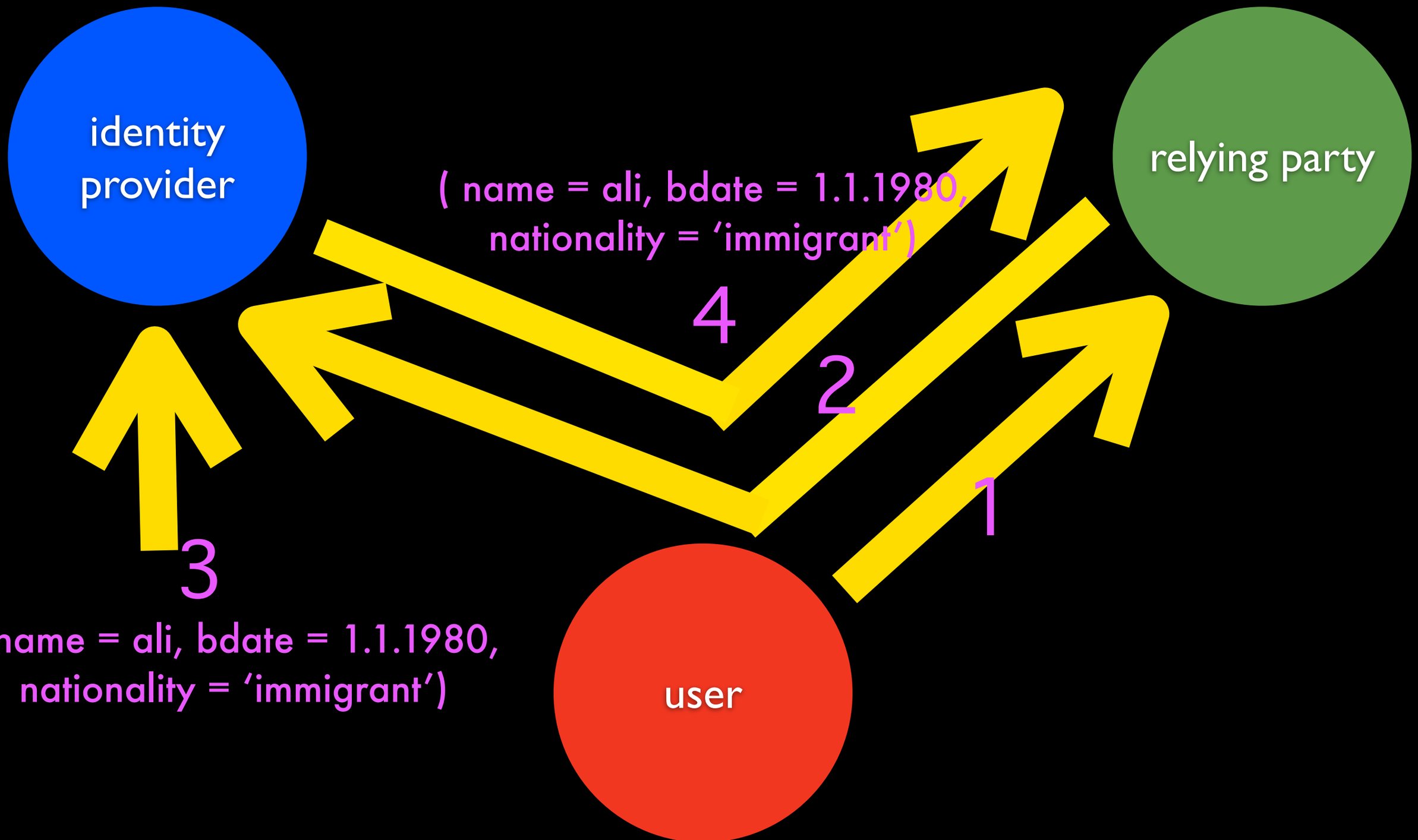
1

3

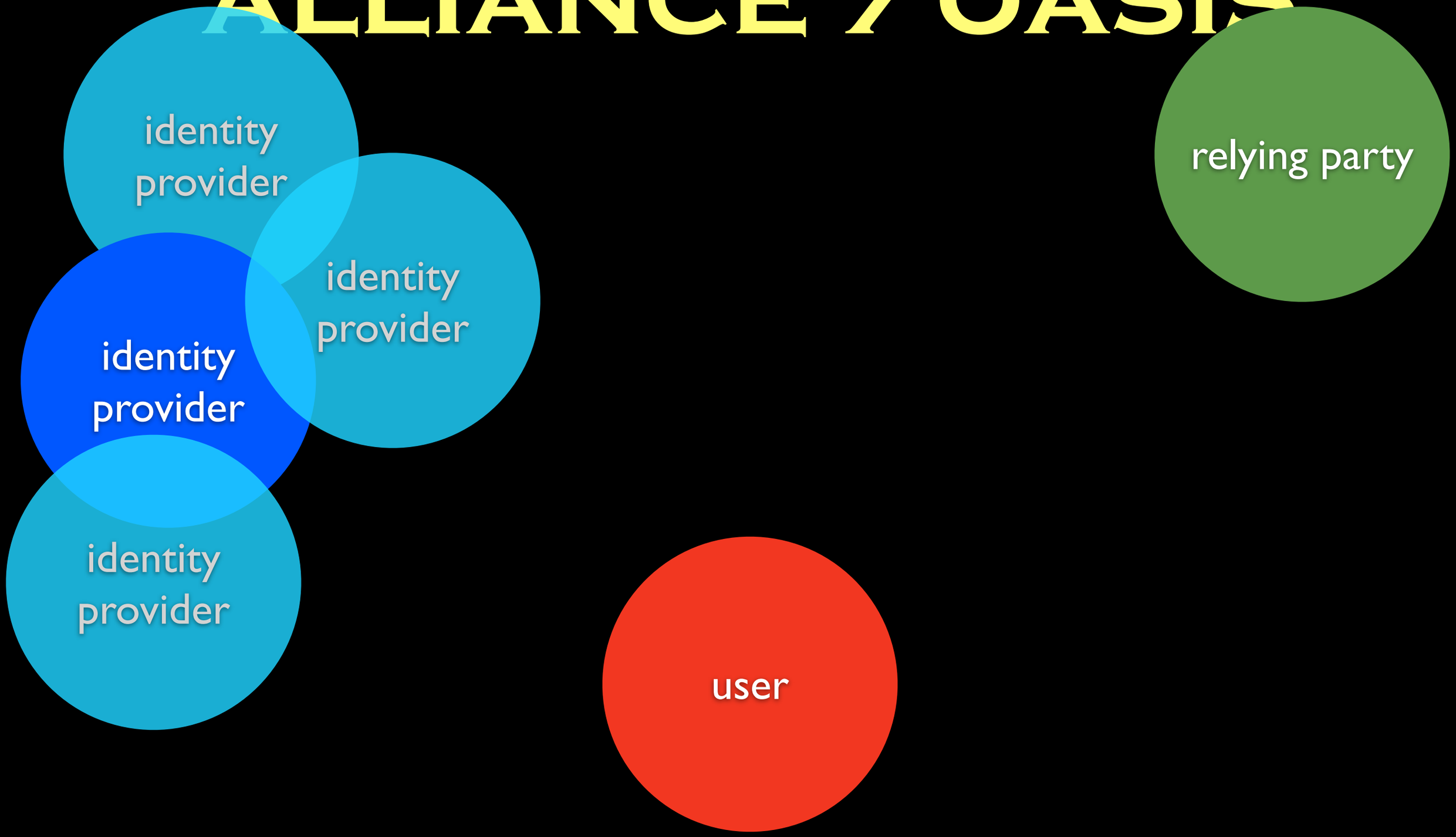
(name = ali, bdate = 1.1.1980,
nationality = ‘immigrant’)

user

SSO


identity provider
relying party
(name = ali, bdate = 1.1.1980,
nationality = 'immigrant')
4
2
1
3
(name = ali, bdate = 1.1.1980,
nationality = 'immigrant')
user

LIBERTY ALLIANCE / OASIS



SELECTIVE DISCLOSURE CREDENTIALS

identity provider

relying party

user

SELECTIVE DISCLOSURE CREDENTIALS

identity provider

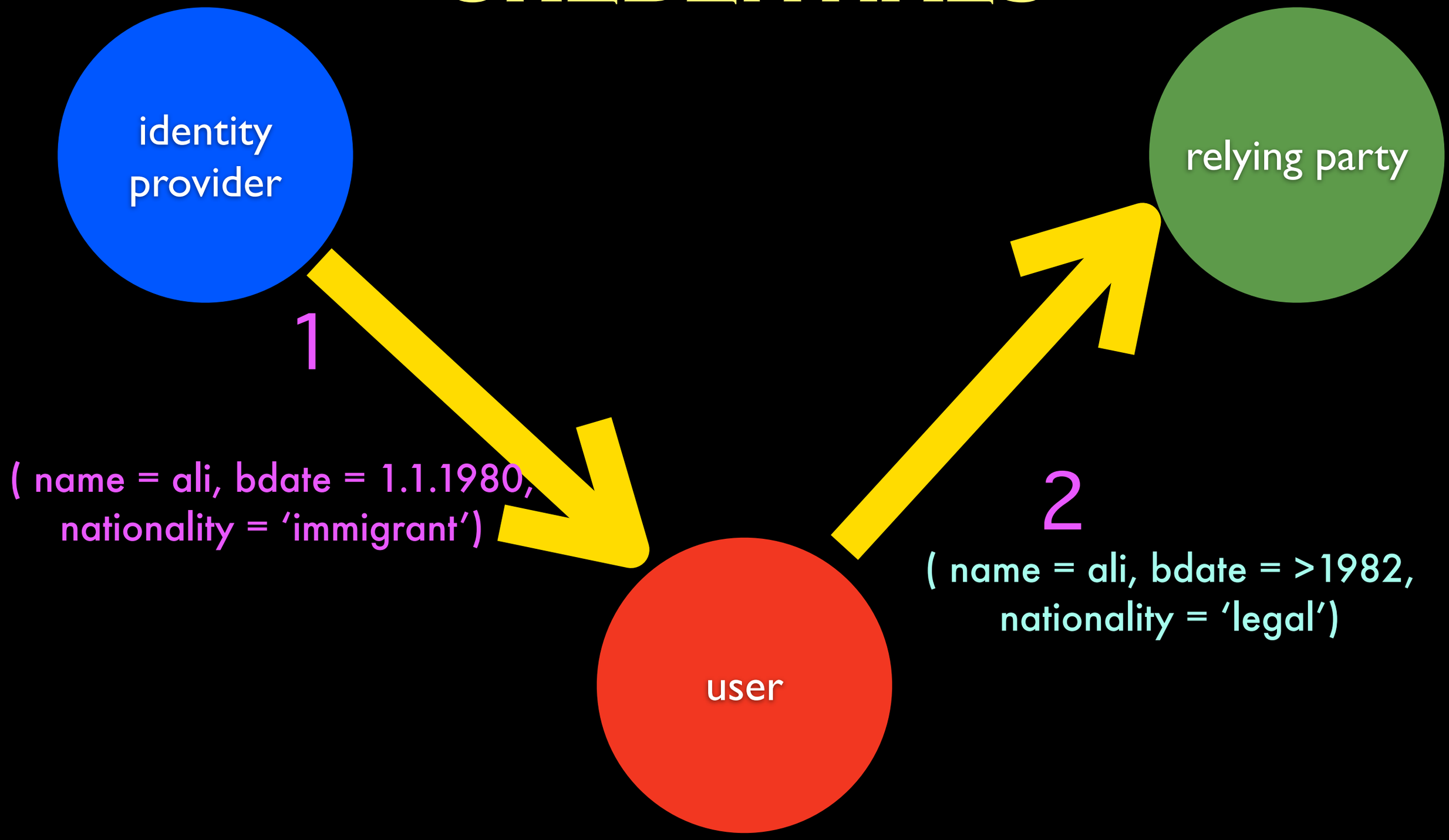
relying party

1

(name = ali, bdate = 1.1.1980,
nationality = ‘immigrant’)

user

SELECTIVE DISCLOSURE CREDENTIALS



ADVANTAGES

★ USER CENTRICITY:

- ✤ UNLINKABLE + UNFORGEABLE
- ✤ PSEUDONYMOUS TRANSACTIONS
- ✤ DISCLOSE SOME CERTIFIED ATTRIBUTES

privacy
as control?

THE REAL PASSPORT

country 1

country 2

1

(name = ali, bdate = 1.1.1980,
nationality = ‘immigrant’,
travelTo = green, purple)

2

(name = ali, bdate = 1.1.1980,
nationality = ‘immigrant’,
travelTo = green, purple)

citizen

THE REAL PASSPORT

country 1

country 2

powerRel1

(name = ali, bdate = 1.1.1980,
nationality = 'immigrant',
travelTo = green, purple)

powerRel2

(name = ali, bdate = 1.1.1980,
nationality = 'immigrant',
travelTo = green, purple)

citizen

will help you with fraud!

government

identity provider

relying party

powerRel3

powerRel1

powerRel2

user

on demand de-annoymization!

government

will help you with fraud!

identity provider

relying party

powerRel3

powerRel1

powerRel2

user

DESIGN FAIL!

- ★ UNIVERSAL IDENTITY SYSTEM
  - ✤ EASY TO CONSTRUCT FRAUD USE CASES
  - ◉ EASY TO JUSTIFY GLOBAL ESCROW
- ★ DISMISSES EXISTING SOLUTIONS
  - ✤ DOUBLE SPENDING PREVENTION
  - ✤ BLACKLISTING WITHOUT DE-ANONYMIZATION
  - ✤ REPUTATION SYSTEMS

government

we do

identity provider

relying party

powerRel3

privacy!

powerRel1

powerRel2

user

relying party

powerRel

user

identity provider

relying party

powerRel

user

relying party

identity provider

identity provider

user

user

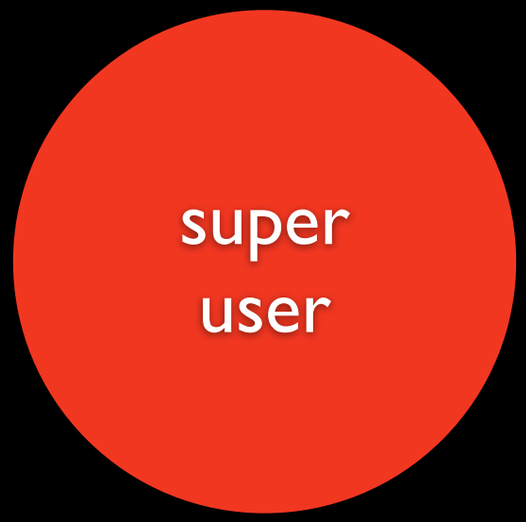
user

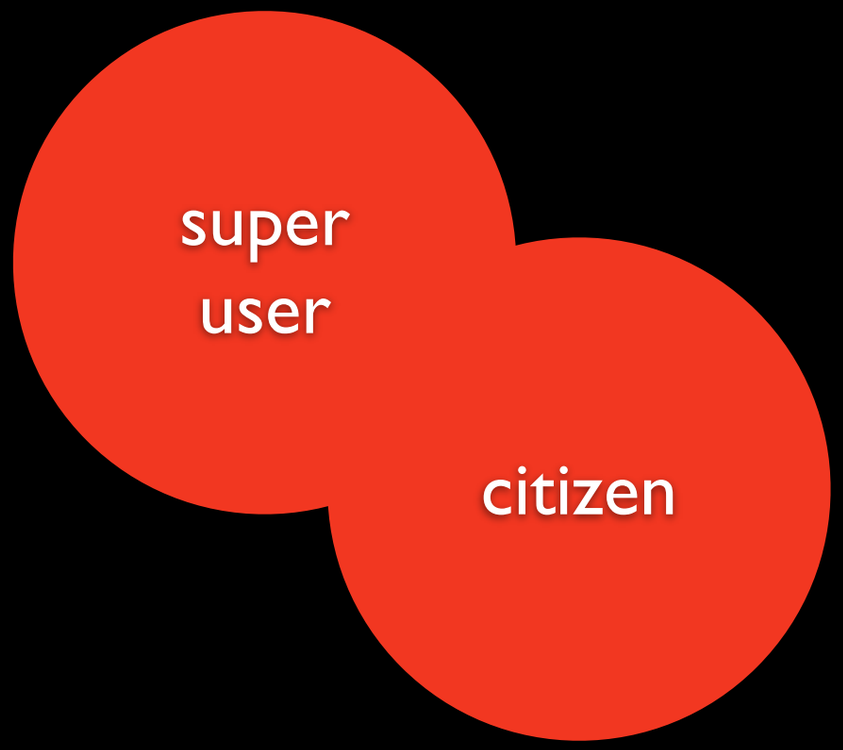
user

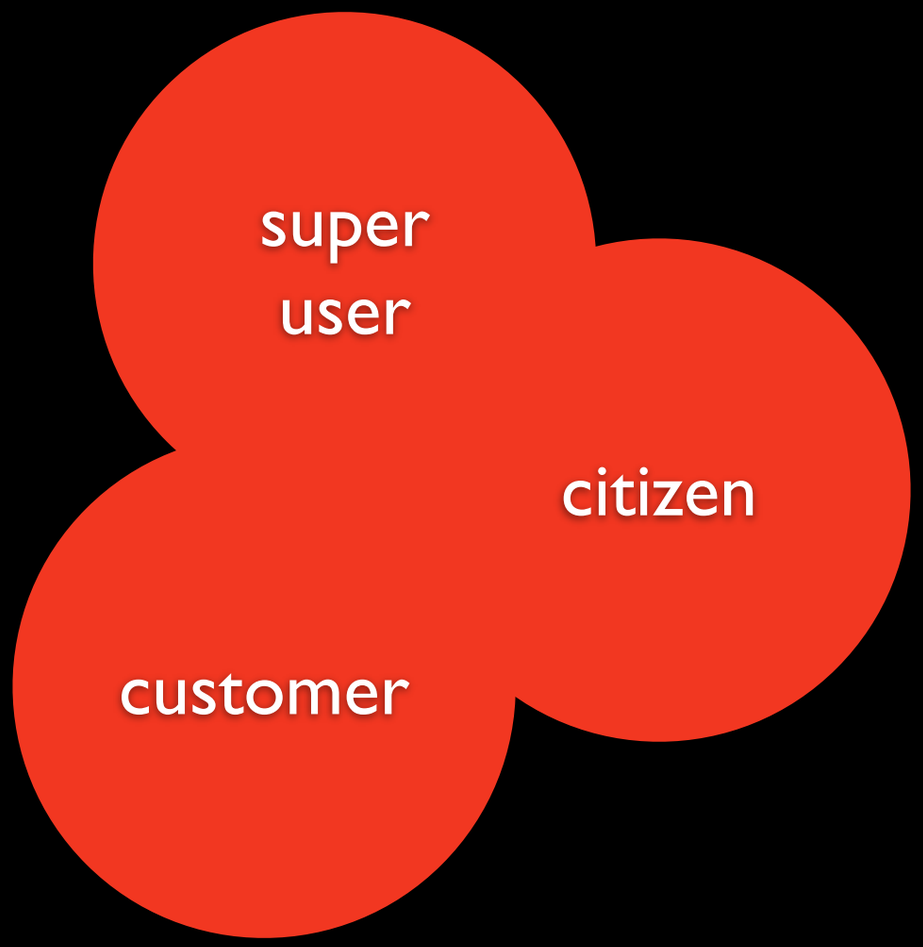
identity provider

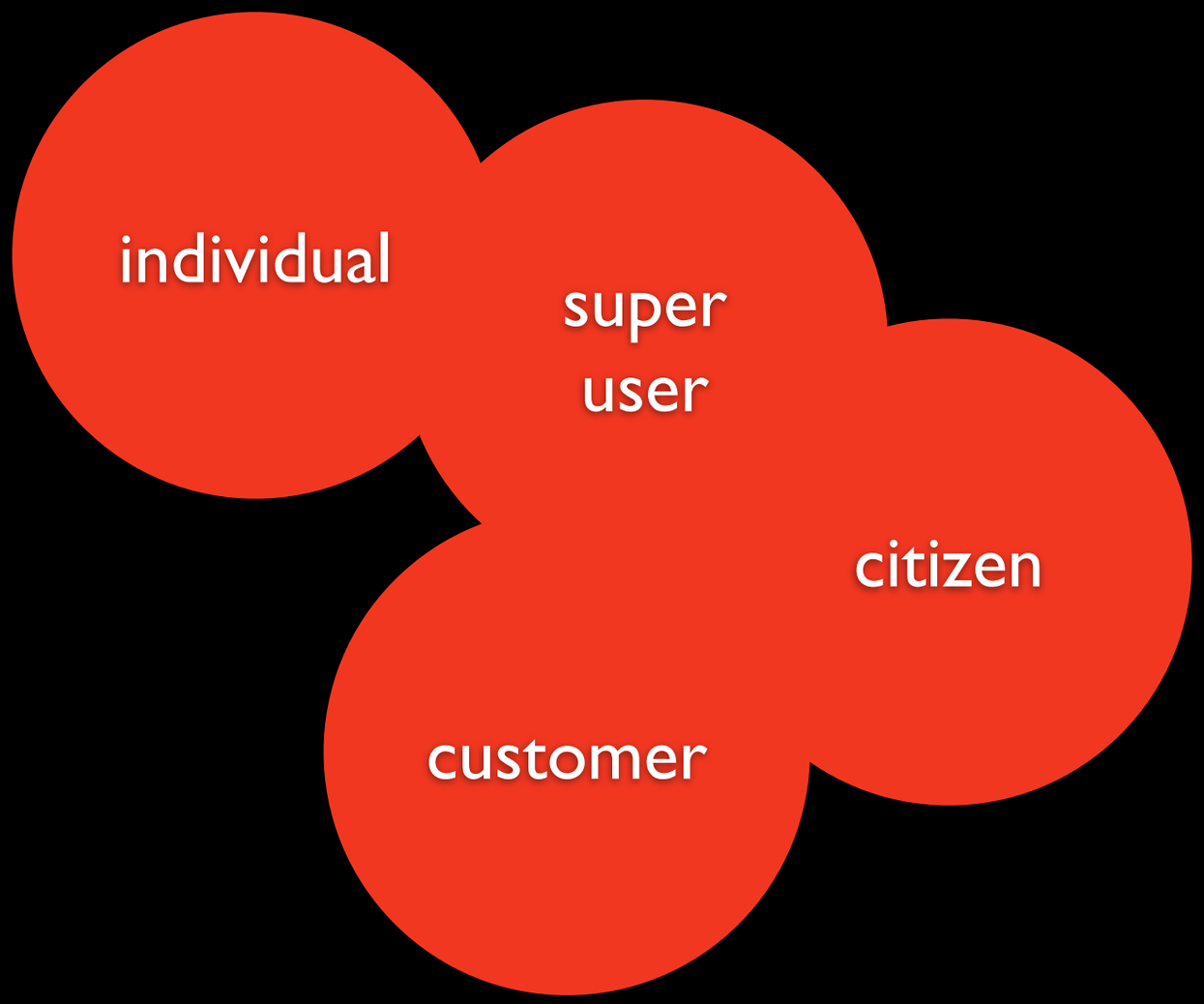
identity provider

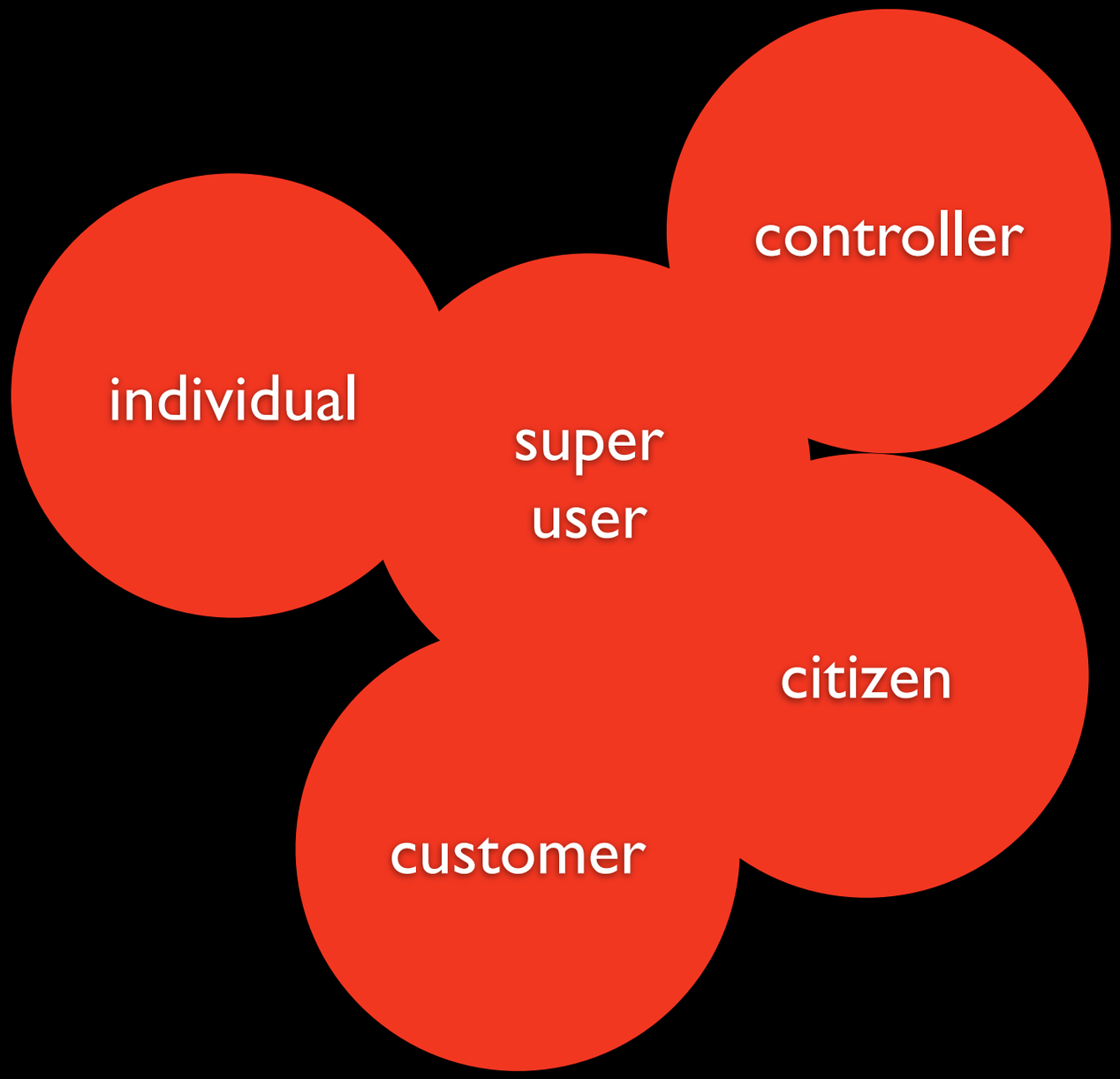
powerRel

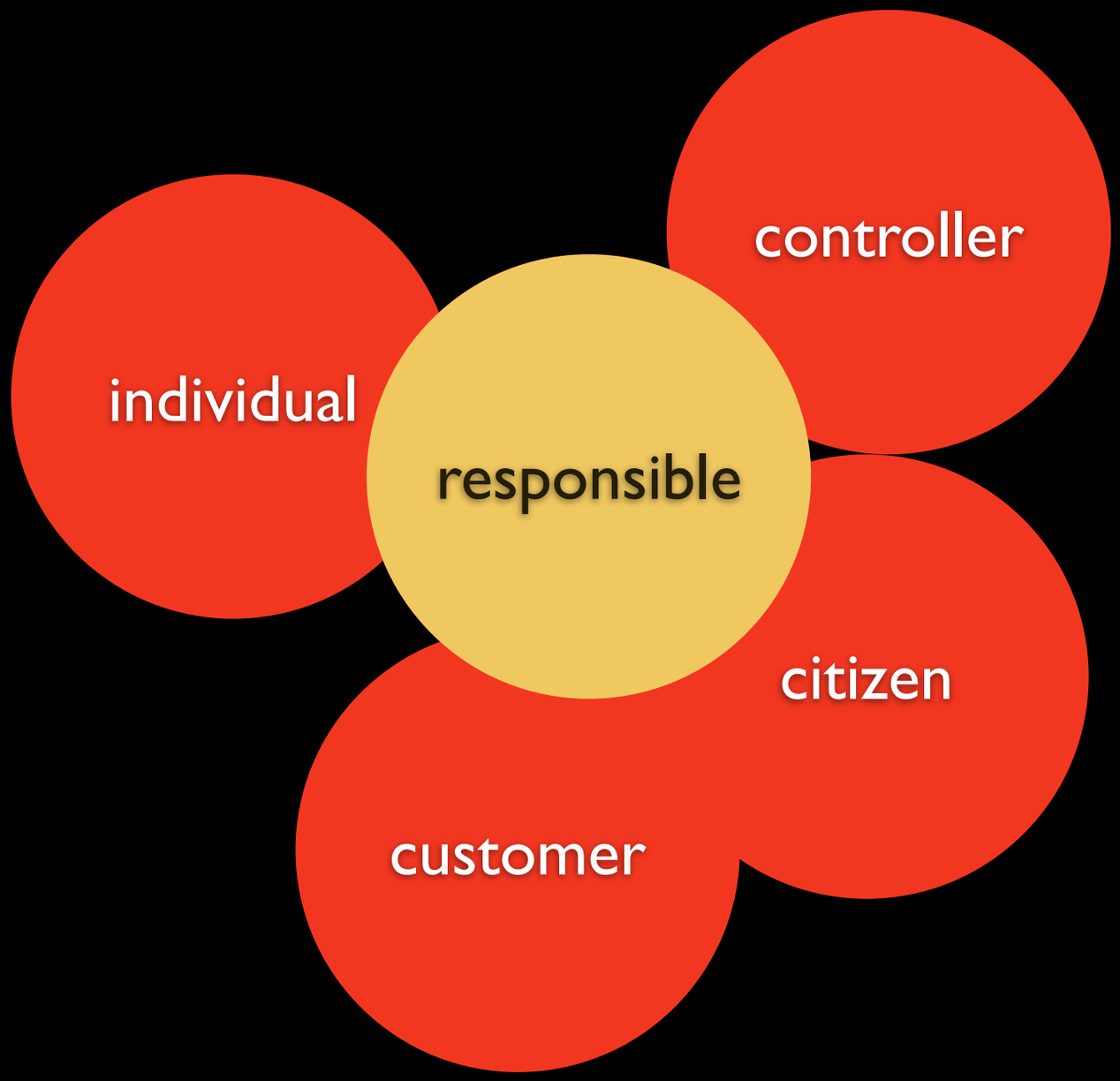

super
user


super
user
citizen

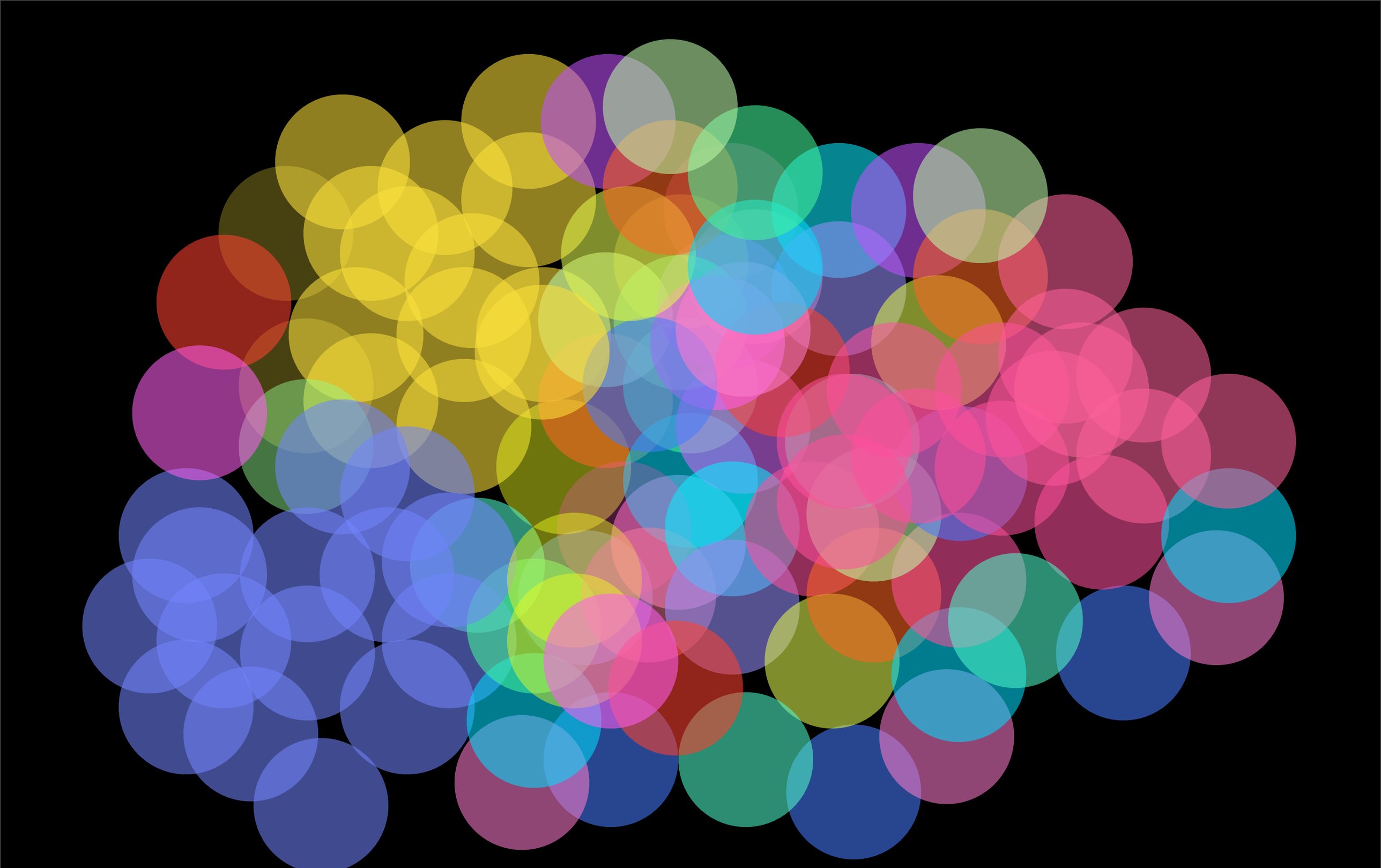

super
user
citizen
customer


individual
super
user
citizen
customer


controller
individual
super
user
citizen
customer


individual
responsible
controller
citizen
customer

privacy
as practice



privacy practices

- MAKE DATA PRACTICES TRANSPARENT
  - DATA MINING ACCESSIBLE AND MANIPULATABLE
  - GAIN AUTHORSHIP IN THE LANGUAGE OF DBS
  - CONTEST THE MEANING OF DATA
    - SEE MICHELLE'S WORK
- ALLOW USERS TO INDIVIDUALLY AND COLLECTIVELY AFFECT THE FLOWS OF INFORMATION
- IDENTITY MIRROR, PRIVACY MIRROR
  - INDIVIDUAL TRANSPARENCY NOT ENOUGH
  - QUESTIONING ECONOMIC THINKING

privacy
as practice?

- ★ USERS MAY WANT TO BE OPEN TO NEGOTIATING PRACTICES
  - ✤ BUT HOW ABOUT SERVICE PROVIDERS AND GOVERNMENTS?
  - ✤ WHO DEFINES WHAT IT MEANS TO BE TRANSPARENT?
- ★ WHICH PRACTICES PREVAIL?
  - ✤ WISDOM OF THE CROWDS?

LESSONS FOR RESEARCHERS AND DEVELOPERS

- AVOID MONOPOLIZING WHAT PRIVACY TECHNICALLY IS:
  - CONFIDENTIALITY
  - CONTROL
  - PRACTICE
  - MAY CREATIVITY PREVAIL...
    - SUICIDE MACHINE
    - PLAYSUREVEILLANCE

LESSONS

- PRIVACY SUBVERTED
  - DATA -> A PERSONAL PROPERTY
  - PRIVACY -> A PRODUCT
  - ATTENTION:
    - PRIVACY PRESERVING SURVEILLANCE?

- ★ FOLLOW PRIVACY TECHNOLOGIES CLOSELY
  - ✤ THE CONSTRAINTS ARE GREATER
  - ✤ THEY NEED TO BE ROBUST
  - ✤ EVALUATE IMPACT
    - ◉ ANECDOTES, ANECDOTES, ANECDOTES

★ PRIVACY IS DEAD

- PRIVACY IS NOT DEAD
  - WE ARE IN THE PROCESS OF CREATING IT...
    - AND NEGOTIATING IT...
      - DON'T FORGET THE COLLECTIVE!

- SEDA@ESAT.KULEUVEN.BE
- WWW.CS.KULEUVEN.BE/~SEDA/