Requirements engineering and privacy by design

Seda Gürses
sguerses@esat.kuleuven.be
Cosic/Esat, K.U. Leuven

★ INTERACTIVE SESSION: HUM IF YOU AGREE...

★ PRIVACY IS AN IMPORTANT FACTOR IN DESIGNING SYSTEMS

★ PRIVACY IS OVER, GET OVER IT!

- USERS DO NOT CARE ABOUT THEIR PRIVACY

- THE USABILITY OF PRIVACY ENHANCING TECHNOLOGIES NEEDS TO BE IMPROVED

- USERS SHOULD TAKE CONTROL OF THEIR DATA

- DATABASE OWNERS SHOULD BE ACCOUNTABLE FOR THE PRIVACY OF THEIR USERS

- USERS KNOW BEST HOW TO HANDLE THEIR PERSONAL DATA

- PRIVACY IS ABOUT A TRADE-OFF: YOU GIVE YOUR PERSONAL DATA FOR UTILITY, SERVICES, COMFORT

- WE CANNOT RELY ON LEGAL MEASURES TO PROTECT PERSONAL DATA

- DATA PROTECTION IS THE BEST SOLUTION WE HAVE TO OUR PRIVACY PROBLEMS

★ THE ONLY THING THAT IS PRIVATE TODAY ARE THE PERSONAL DATA SILOS AND THE DATA MINING METHODS USED IN THEM TO DISCRIMINATE PEOPLE/ CUSTOMERS/CITIZENS.

- SECURITY ENGINEERS, SOFTWARE DEVELOPERS AND LEGAL EXPERTS HAVE INSIGHT INTO PRIVACY RISKS THAT NORMAL USERS DO NOT

- THEREFORE, SECURITY ENGINEERS, SOFTWARE DEVELOPERS AND LEGAL EXPERTS SHOULD DESIGN PRIVACY ENHANCING SYSTEMS

- SOCIAL NETWORK SITES ARE A PRIVACY NIGHTMARE

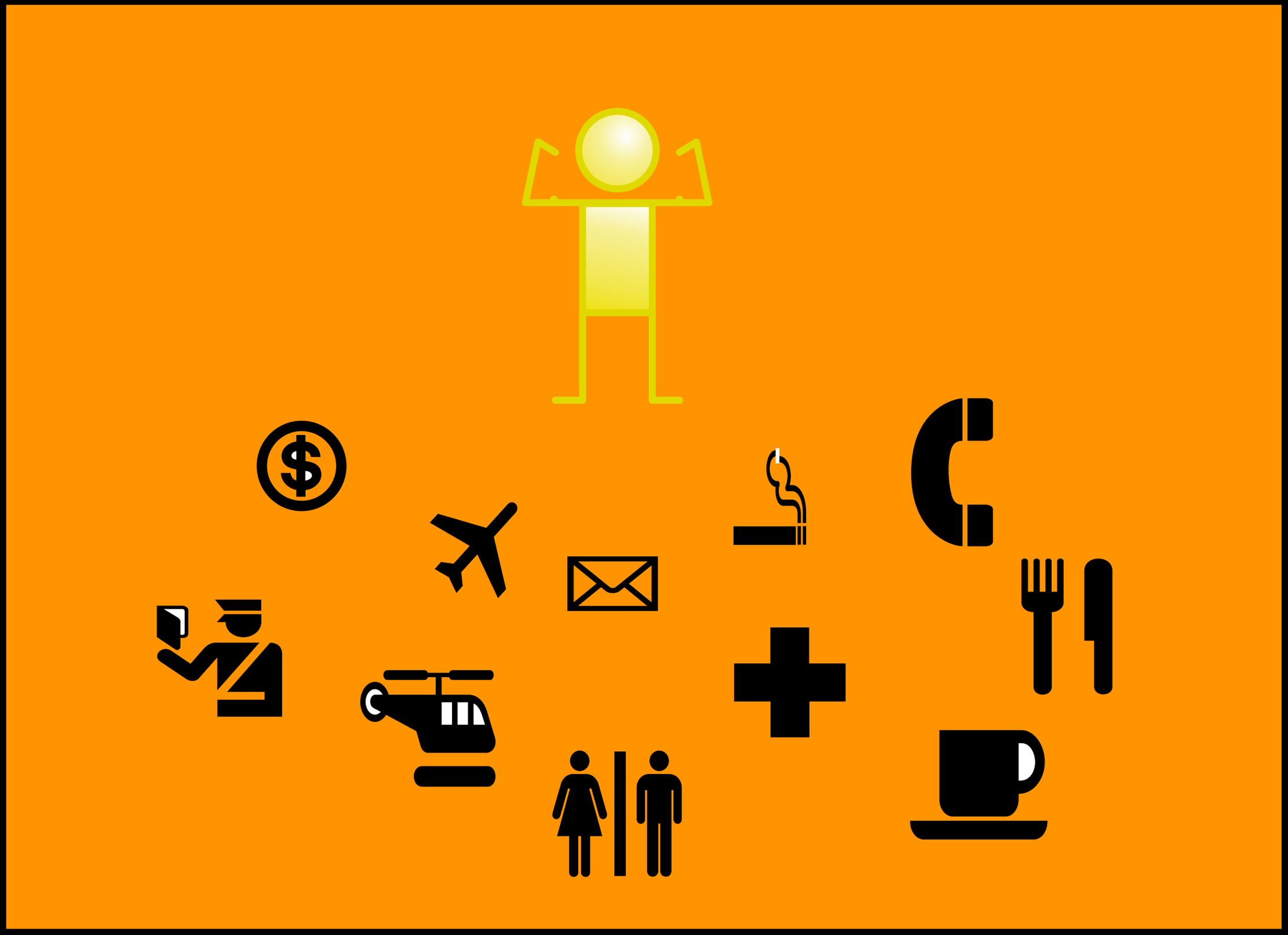
- SOCIAL NETWORK SITE PROVIDERS ALLURE THEIR USERS INTO GIVING UP THEIR PRIVACY

- SOCIAL NETWORK SITE ARE THE MOST ADVANCED IDENTITY MANAGEMENT SYSTEMS THAT WE HAVE

- SOCIAL NETWORKS USERS GIVE UP THEIR PRIVACY

★ PROBLEM: Design a system

- ✤ WHY?
  - ◉ privacy is a concern
- ✤ WHAT?
  - ◉ A SYSTEM THAT IS PRIVACY ...
    - ✳ PRESERVING
    - ✳ ENHANCING
    - ✳ AWARE ...
- ✤ HOW?



DATA COLLECTION

DATA PROCESSING

DATA DISSEMINATION

DATA DELETION

100%

personal data

0%

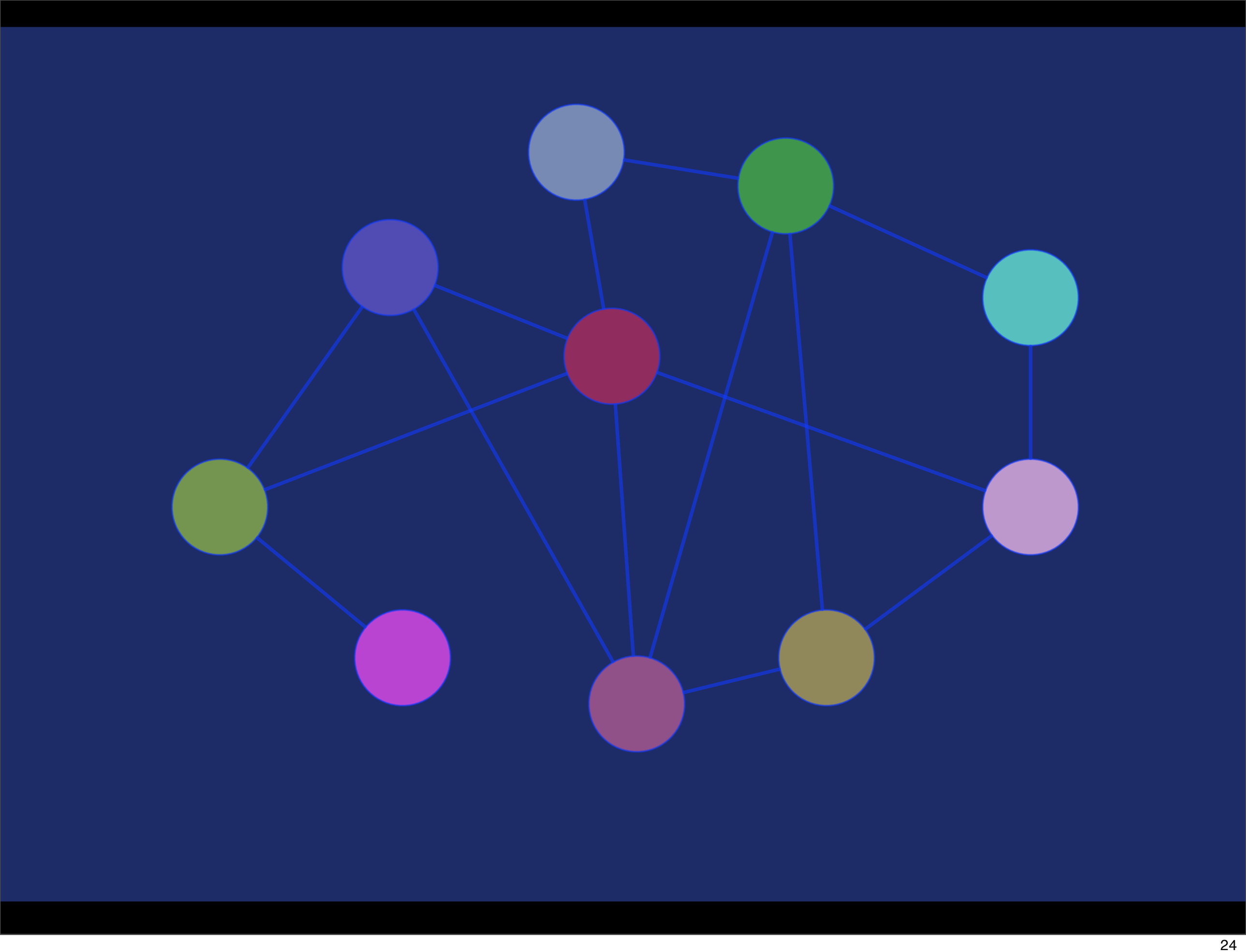
CONFIDENTIALITY

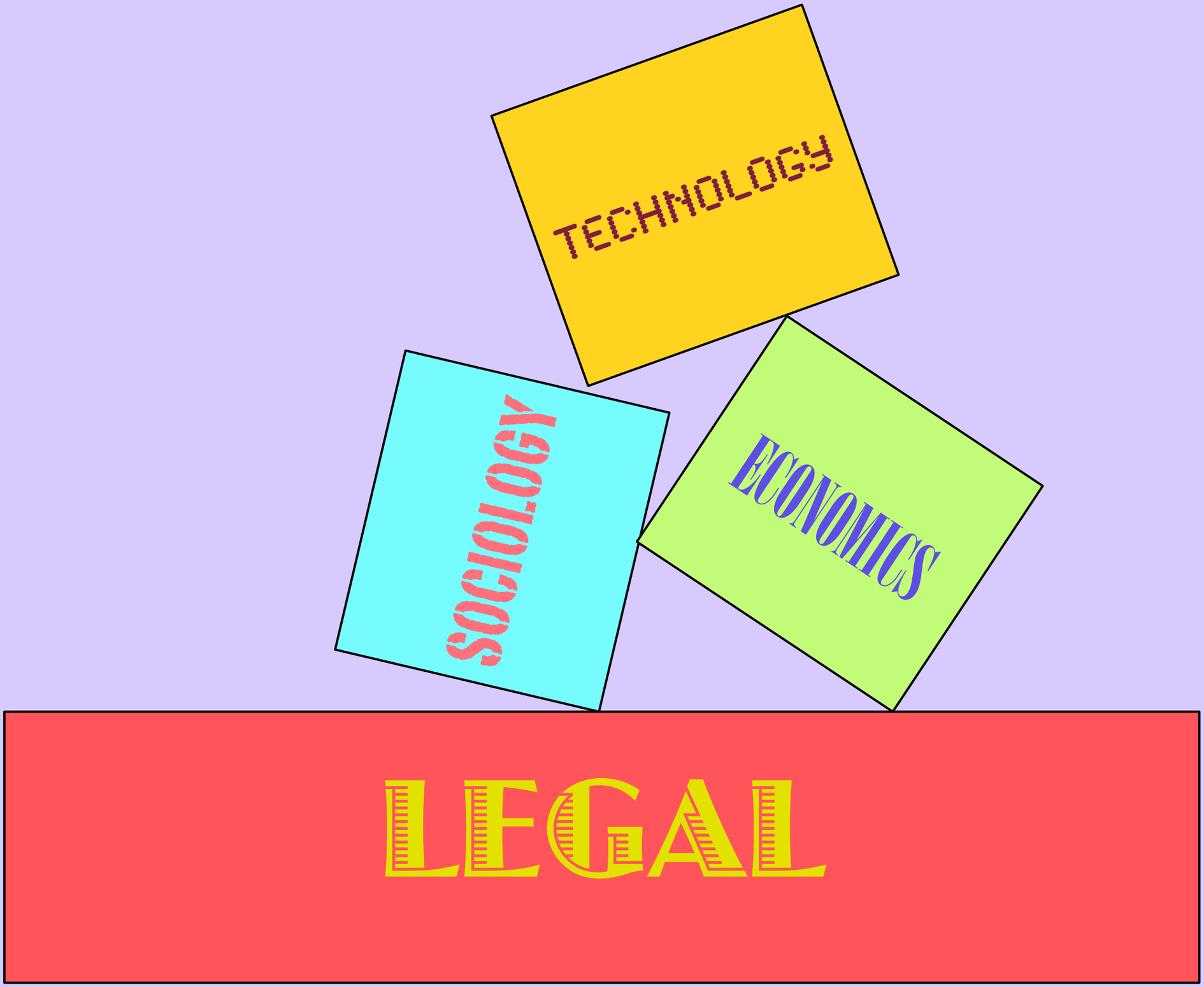
transparency

ANONYMITY

pseudonymity

data protection




TECHNOLOGY
SOCIOLOGY
ECONOMICS
LEGAL

PRIVACY PRINCIPLES

- ★ FAIR AND LAWFUL PROCESSING
- ★ CONSENT
- ★ PURPOSE SPECIFICATION
- ★ MINIMALITY
- ★ MINIMAL DISCLOSURE
- ★ INFORMATION QUALITY
- ★ DATA SUBJECT CONTROL
- ★ SENSITIVITY
- ★ INFORMATION SECURITY

DATA SUBJECT RIGHTS

- ACCESS TO PERSONAL DATA
- OBJECT TO DATA PROCESSING
- DELETE PERSONAL DATA
- UPDATE/DELETE INACCURATE DATA
- PREVENT NON-CONSENTED USE/PURPOSE

CATEGORIES AND TYPOLOGIES OF DATA

- ★ PERSONAL DATA
  - ✣ CAN BE USED TO IDENTIFY A PERSON
- ★ SENSITIVE DATA
  - ✣ BELIEFS, OPINIONS, AFFILIATION, HEALTH, RACE
- ★ IDENTIFICATION DATA
  - ✣ DATA FOR DIRECT IDENTIFICATION OF DATA SUBJECTS
- ★ ANONYMOUS DATA (NOT REGULATED BY DP)
  - ✣ NO IDENTIFIED OR IDENTIFIABLE SUBJECT

ACTORS

- DATA SUBJECT
- DATA CONTROLLER
- DATA PROCESSOR
- PERSONS IN CHARGE OF PROCESSING
- 3. PARTY
- RECIPIENT
- PRIVACY AUTHORITY
  - SET RESPONSIBILITIES AND POWERS IMPOSED BY DP

PURPOSE

- RATIONALE OF THE PROCESSING
- ESTABLISHES BOUNDARIES
- CAN BE ORGANIZED IN A HIERARCHICAL STRUCTURE
  - DATABASE OF PURPOSES
  - TREES OR HYPERGRAPHS

CONSENT

- MANIFESTS THE DATA SUBJECT'S VOLITION TO ALLOW DATA CONTROLLER TO PROCESS HER PERSONAL DATA
  - CONSENT ≈ PERMISSION
  - CONSENT ≈ PRECONDITION FOR DELEGATION OF RIGHTS

CONSENT

- ★ DATA SUBJECT CAN WITHDRAW CONSENT
- ✤ REVOCATION MODELS
  - ◉ DEEP REMOVAL
  - ◉ SHALLOW REMOVAL

OBLIGATION

- A CONDITION OR ACTION TO BE PERFORMED BEFORE OR AFTER AN ACTION IS TAKEN
- NECESSARY FOR IMPLEMENTATION

OBLIGATION

- OBLIGATION POLICY
  - AUTHENTICATION + AUTHORIZATION NOT ENOUGH
  - DEFINE ACTIONS THAT HAVE TO BE TAKEN WHEN PERMISSIONS ARE GRANTED
- DEONTIC LOGIC
  - OBLIGATIONS ENTAIL PERMISSIONS
- OTHER CLASSIFICATIONS:
  - PROVISIONS (BEFORE ACTION)
  - OBLIGATIONS (DURING/AFTER ACTION)

RETENTION PERIOD

- DELETE, DESTROY, OR ANONYMIZE DATA ONCE PROCESSING FOR A PURPOSE IS COMPLETED
  - COMPLEX MATTER:
    - GUARANTEES NOT POSSIBLE
    - LOGS/BACKUPS
    - SEE ALSO REVOCATION MODELS

PRIVACY ENGINEERING

- A SYSTEMATIC EFFORT TO EMBED PRIVACY RELEVANT LEGAL PRIMITIVES INTO TECHNICAL AND GOVERNANCE DESIGN
  - SPECIFY PRIVACY PROMISES
  - GUARANTEE THEIR ENFORCEMENT
  - COMPLY WITH DP LEGISLATION

PRIVACY ENGINEERING

- ORGANIZATION'S PRIVACY PRACTICES HAVE TO BE DOCUMENTED SO THAT INDIVIDUALS CAN WIELD THEIR RIGHTS
  - PURPOSES AND MODALITIES OF THE PROCESSING
  - OBLIGATORY/VOLUNTARY DATA REQUESTS
  - CATEGORIES AND TYPOLOGIES OF DATA
  - THE RECIPIENTS/CATEGORIES OF RECIPIENTS
  - THE RIGHTS OF DATA SUBJECTS

POLICY LANGUAGES

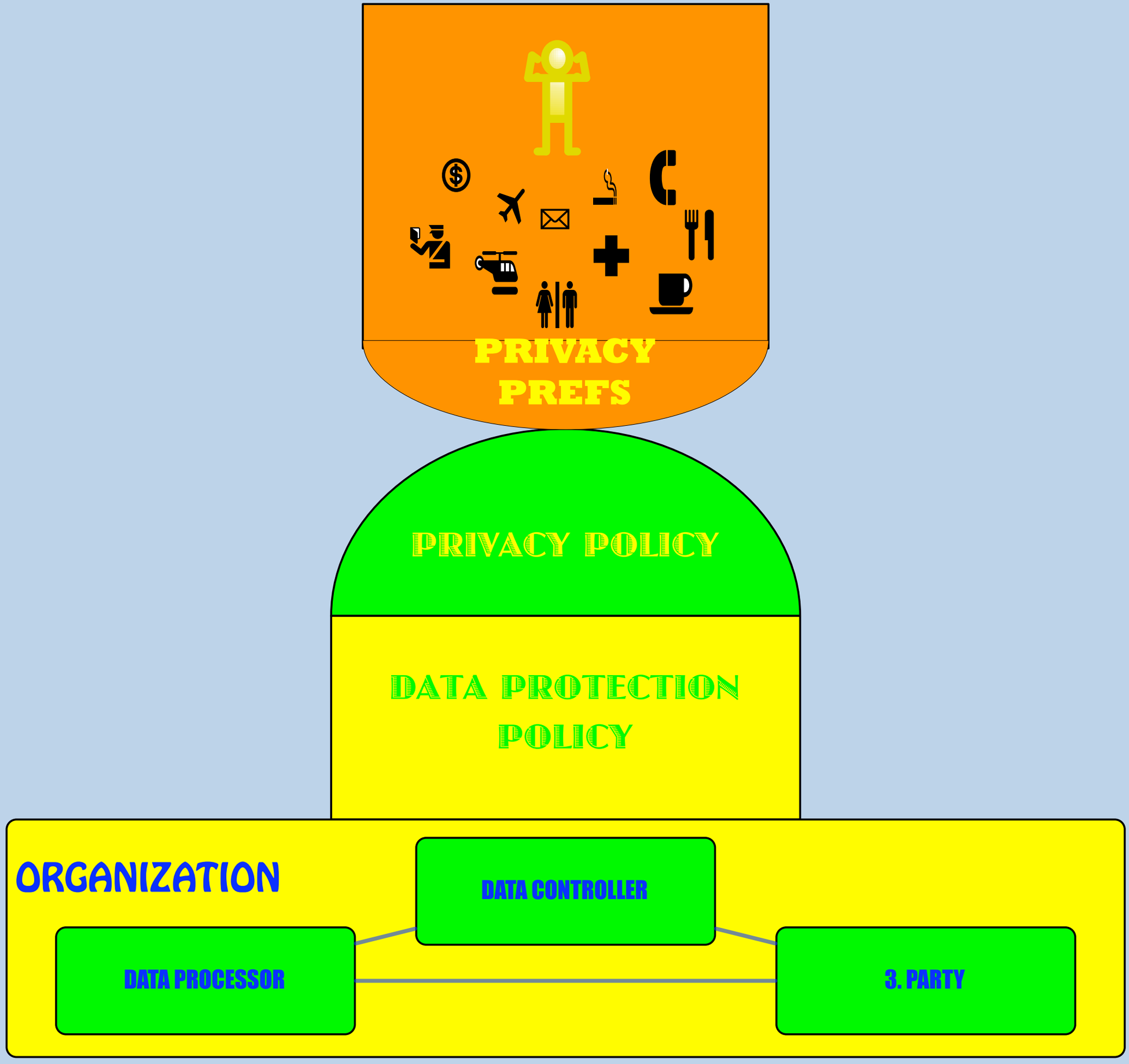
- ★ P3P (PLATFORM FOR PRIVACY PREFERENCES)
  - ✤ W3C STANDARD
  - ✤ ENABLES WEB SITES TO EXPRESS THEIR DATA COLLECTION AND DATA USE PRACTICES
    - ◉ MACHINE READABLE XML
    - ◉ CAN BE RETRIEVED AUTOMATICALLY
    - ◉ INTERPRETED EASILY BY USERS

APPEL

- P3P PREFERENCE LANGUAGE
  - A SET OF RULES THAT EVALUATE TO A JUDGEMENT ABOUT MATCHING PREFERENCES AND POLICIES
    - REQUEST ACCESS
    - LIMITED
    - BLOCK

P3P + APPEL

- DRAWBACKS
  - ORIGINALLY SPECIFY WHAT IS UNACCEPTABLE
  - AMBIGUOUS AND AWKWARD
  - LACK OF WELL DEFINED SEMANTICS
  - UNABLE TO REPLICATE HUMAN READABLE POLICY
  - HENCE LEGAL UNCERTAINTY


PRIVACY
PREFS
PRIVACY POLICY
DATA PROTECTION
POLICY
ORGANIZATION
DATA CONTROLLER
DATA PROCESSOR
3. PARTY

PRIVACY ENGINEERING METHOD

- ★ MUST INCLUDE:
  - ✤ CAPTURE THE STRUCTURE OF ORGANIZATIONS AND THEIR ENVIRONMENTS
  - ✤ CAPTURE THE PURPOSES FOR WHICH PERSONAL DATA ARE COLLECTED
    - ◉ LINK PERMISSIONS TO THEM
  - ✤ IDENTIFY THE KIND OF DATA INVOLVED IN PROCESSING
  - ✤ CAPTURE THE OBLIGATIONS AND LINK TO PERMISSION

PROBLEMS?

PROBLEMS?

- WITHOUT DATA PROTECTION COMPLIANCE NO PRIVACY AWARE SYSTEM
- BUT, IS WITH DATA PROTECTION COMPLIANCE A SYSTEM PRIVACY AWARE?

DP fail: Facebook

- ★ Facebook's privacy policy is compliant
  - ✤ TRUSTe certification
    - ◉ Privacy and data protection policy aligned
    - ◉ Hundreds of privacy preferences
  - ✤ Purpose definition includes everything
- ★ A privacy aware system?

TECHNICAL COMPLEXITY

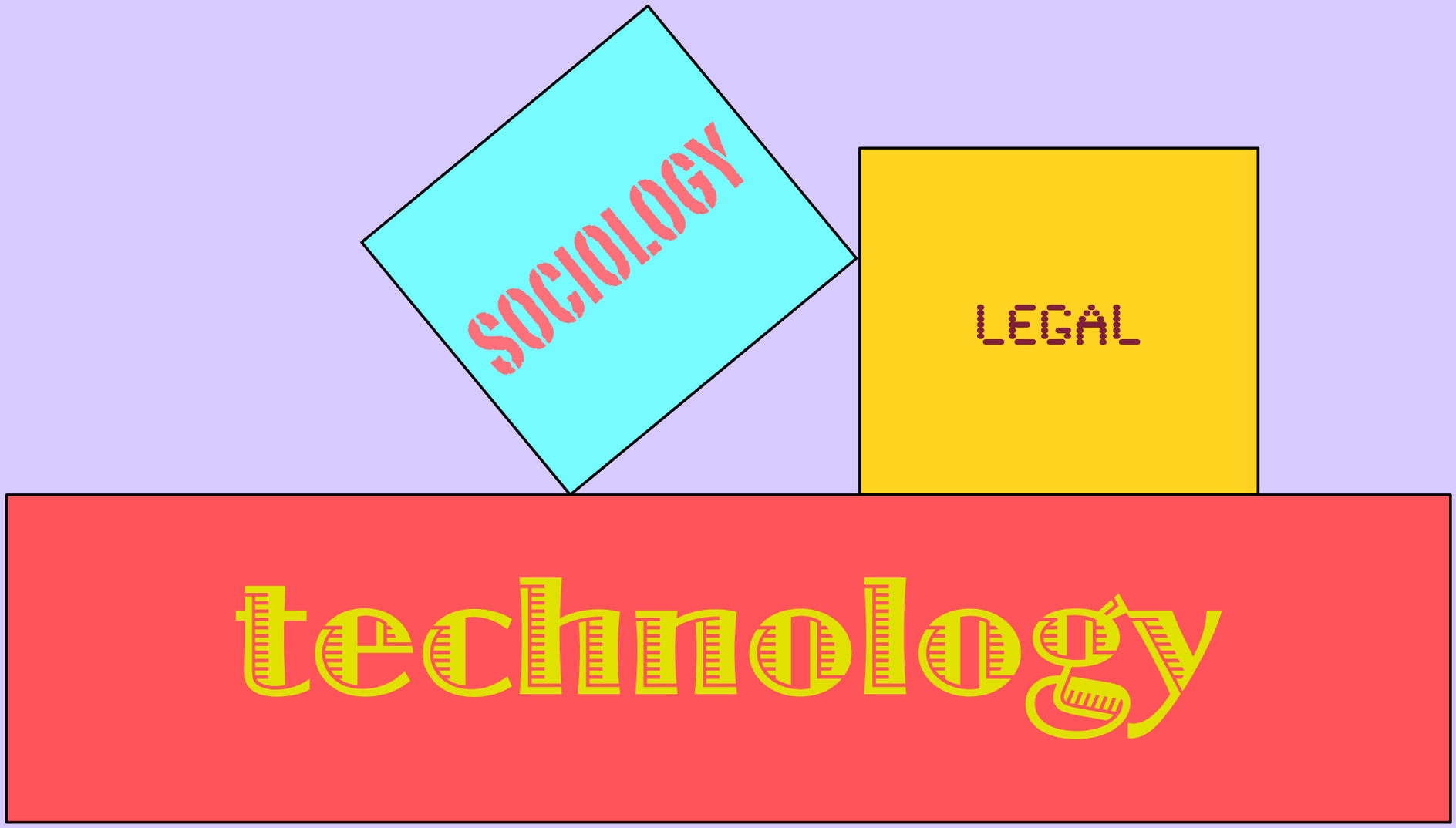
- HOW MANY CONSENTS?
- HOW OFTEN?
- HOW MANY PRIVACY POLICIES TO MANAGE?
- HOW OFTEN TO CONTROL DATA
- AUTOMATION:
  - WHO IS THEN RESPONSIBLE WHEN THINGS GO WRONG?

USER OVERLOAD

- MANU LUKSCH'S PROJECT FACELESS
  - DOZENS OF REQUESTS FOR DATA SUBJECT ACCESS RIGHT
    - PERSONAL DATA = LEGAL READY-MADES
      - OVER 90% REJECTED

INFERENCES

- NO PROPER INFERENCE ANALYSIS
  - A IS NOT REVEALED, BUT INFERRED FROM B AND C
    - DATA SUBJECT CONSENTS TO B AND C
- ANONYMIZED DATA
  - WHERE IS THE LIMIT?
  - AGGREGATION OF DATA
  - CATEGORIZATION AND DISCRIMINATION

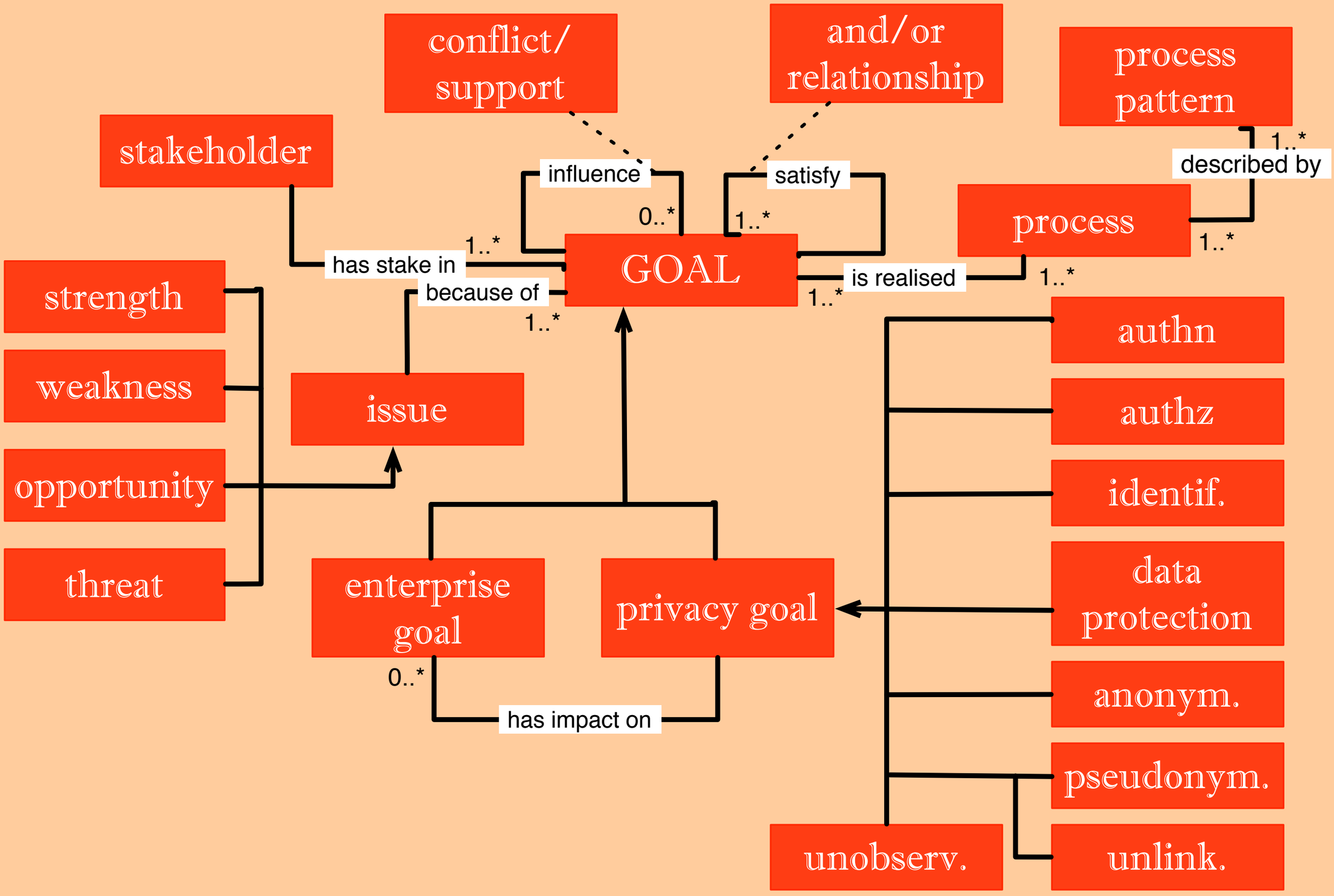

SOCIOLOGY
LEGAL
technology

PRIVACY REQUIREMENTS

- ★ IDENTIFICATION
- ★ AUTHENTICATION
- ★ AUTHORISATION
- ★ DATA PROTECTION
- ★ ANONYMITY
- ★ PSEUDONYMITY
- ★ UNLINKABILITY
- ★ UNOBSERVABILITY

PRIVACY REQUIREMENTS INTO SYSTEM DESIGN

- ANALYZE IMPACT OF PRIVACY REQUIREMENTS ON ORGANISATIONAL GOALS
- SUGGEST APPROPRIATE SYSTEM IMPLEMENTATION TECHNIQUES FOR REALISING REQUIREMENTS
  - PETS

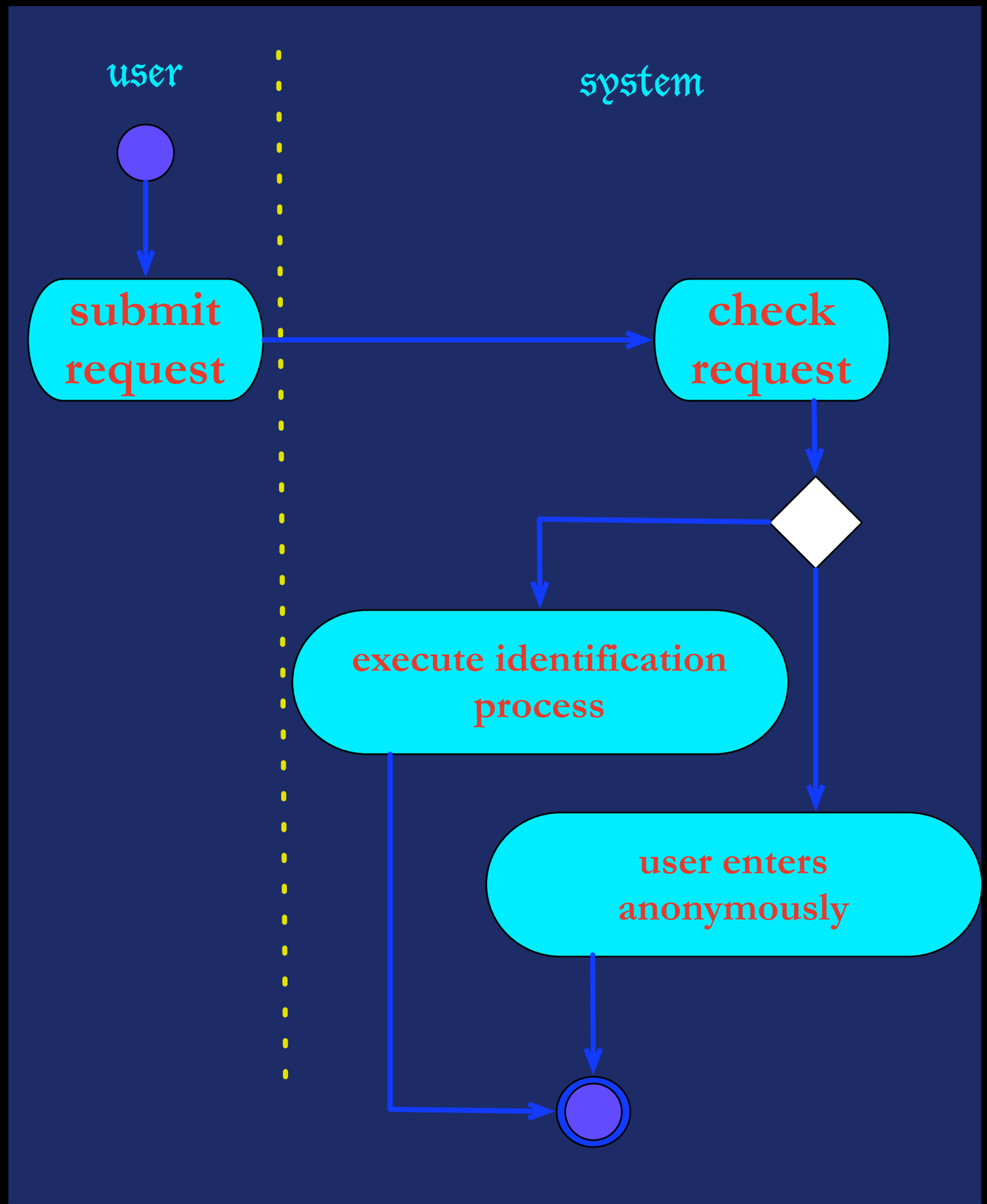

conflict/ support
and/or relationship
process pattern
stakeholder
influence
satisfy
1..*
described by
0..*
1..*
process
1..*
1..*
has stake in
GOAL
is realised
1..*
because of
1..*
strength
authn
weakness
issue
authz
opportunity
identif.
threat
enterprise goal
privacy goal
data protection
0..*
anonym.
has impact on
pseudonym.
unobserv.
unlink.

METHOD - 1

- ELICIT PRIVACY RELATED GOALS
  - FUNCTIONAL REQUIREMENTS STAND
  - AGREE WITH STAKEHOLDERS
- ANALYSE THE IMPACT OF PRIVACY GOALS ON ORGANISATIONAL PROCESS
  - MAY LEAD TO NEW GOALS OR ADAPTATION
  - SEARCH ALTERNATIVES
    - AND/OR GOAL HIERARCHY

METHOD - 2

- MODEL AFFECTED PROCESSES USING PRIVACY PROCESS PATTERNS



METHOD - 3

- IDENTIFY TECHNIQUES THAT BEST SUPPORT/IMPLEMENT THE ABOVE PROCESS
  - DEFINE SYSTEM ARCHITECTURE

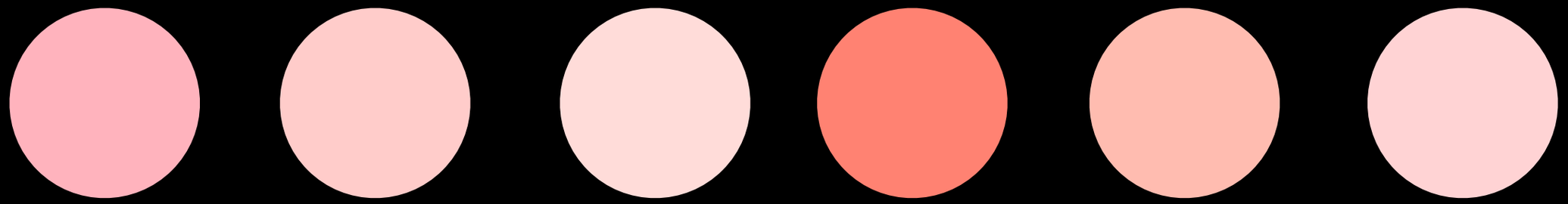
ADVANTAGES OF METHOD

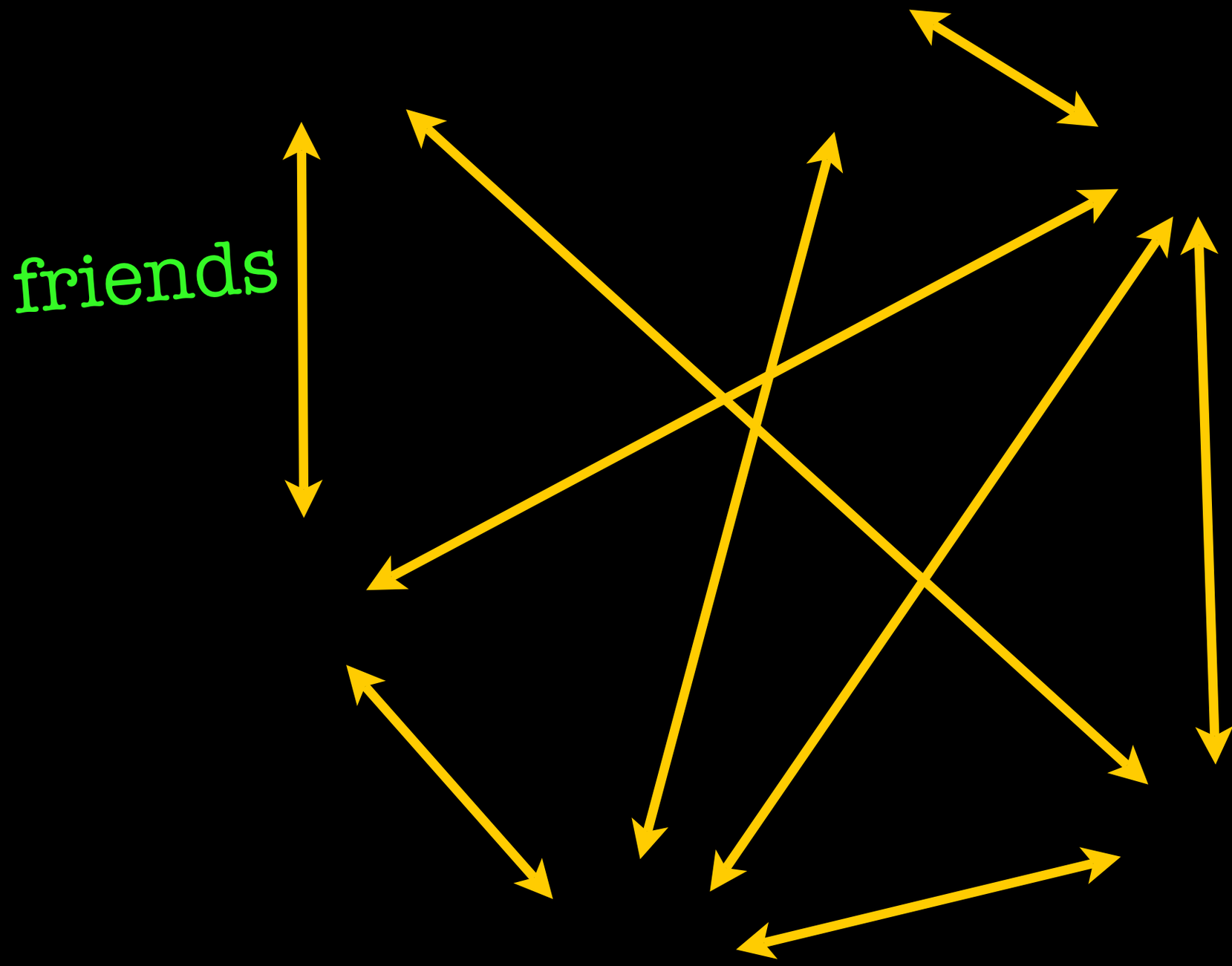
- ★ SYSTEMATICALLY THINK ABOUT WHERE TO PLUG IN EXISTING SOLUTIONS
- ✤ PETS
- ✤ DATA PROTECTION
- ✤ THINK ABOUT INTERFACES FOR ANONYMOUS/UNOBSERVABLE/UNLINKABLE ACCESS

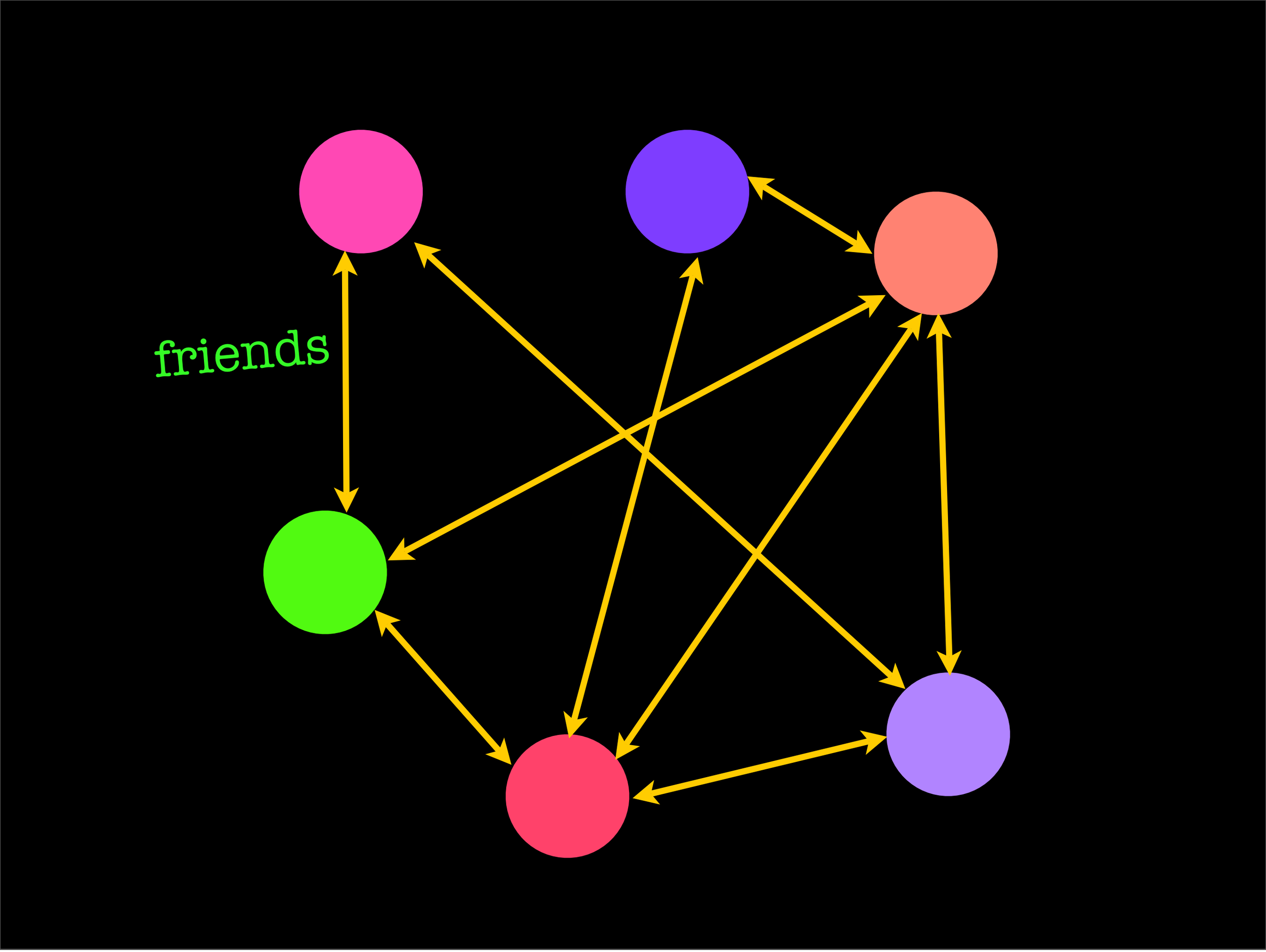
PROBLEMS?

PROBLEMS?

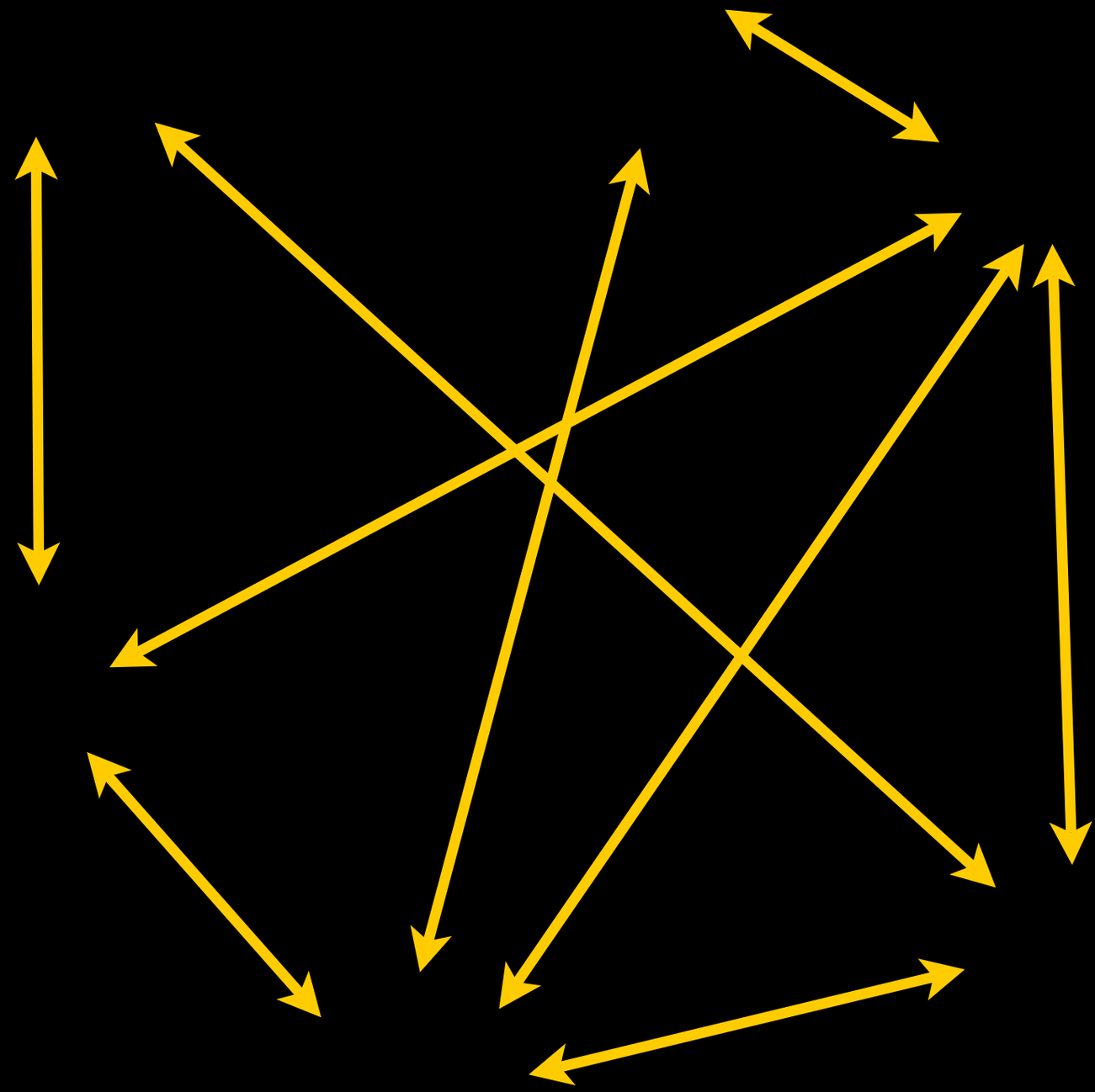
- ★ INFERENCE ANALYSIS IGNORED
- ★ NO CONSIDERATION OF STORED DATA
- ★ DATA PROTECTION VERY SUPERFICIAL
- ★ PROCESS PATTERNS TOO SIMPLISTIC/ DECONTEXTUALIZED
- ★ FOCUS ON INDIVIDUAL DATA CONTROL



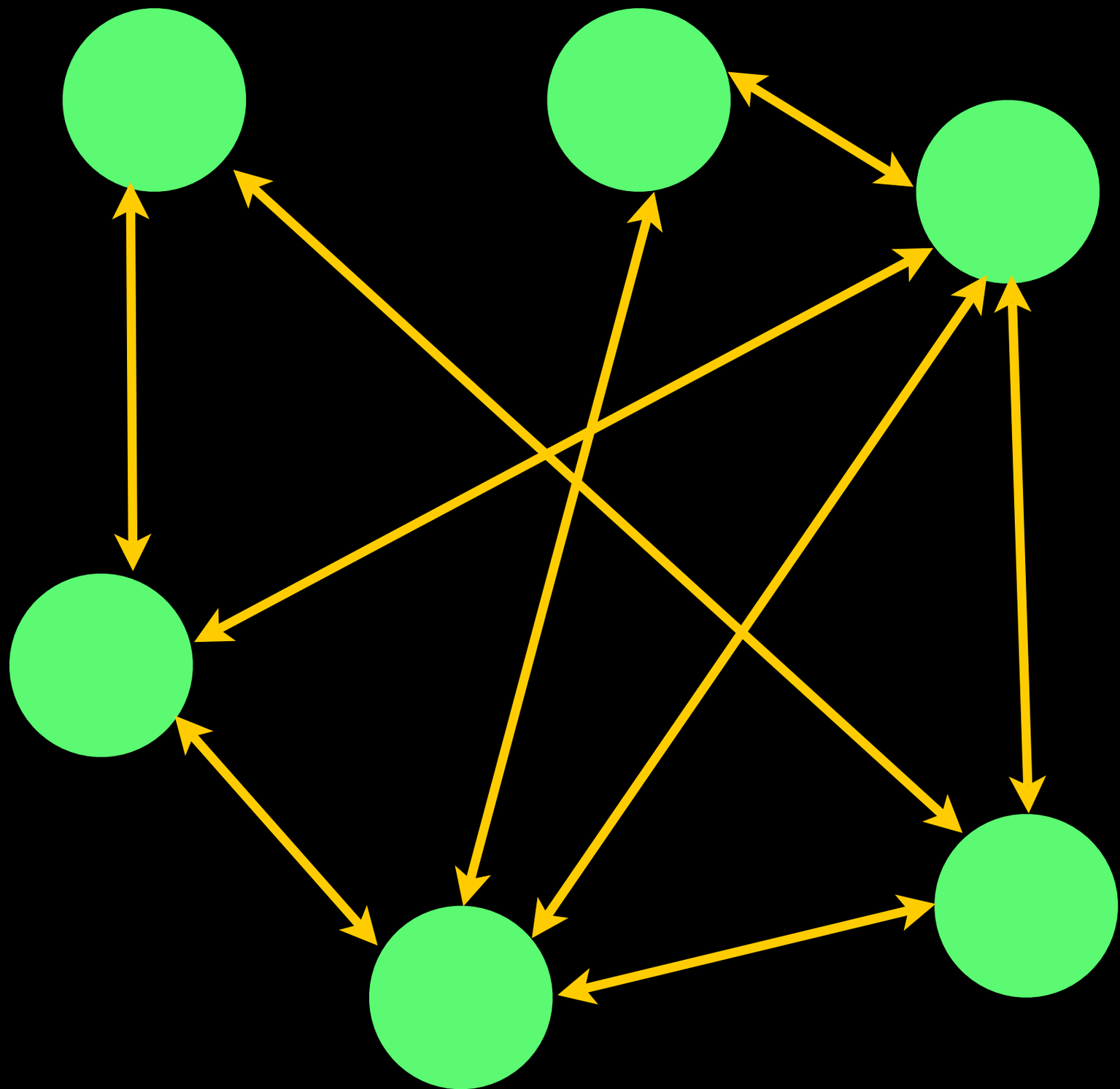

friends


friends

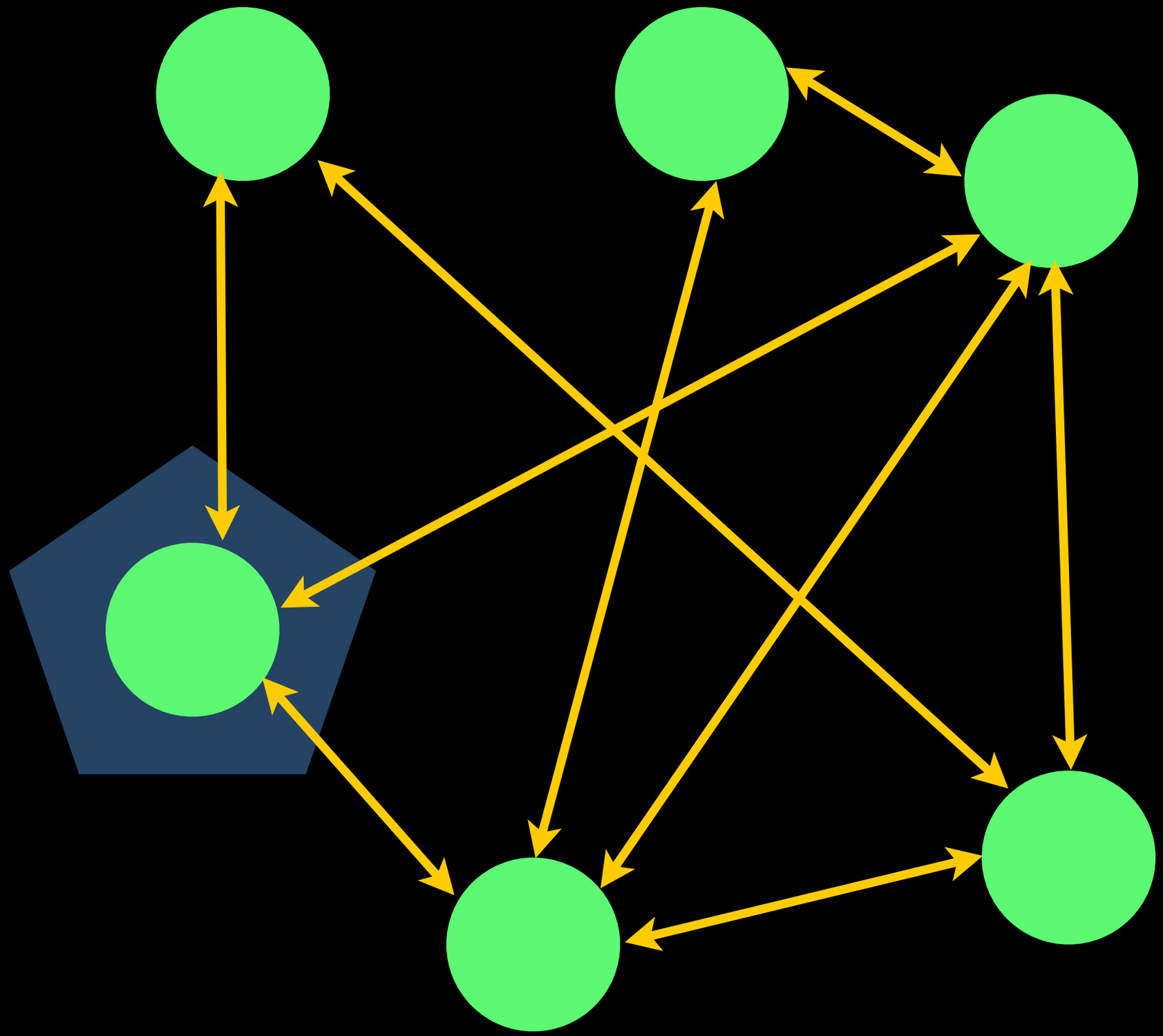
joe has 3 friends, alice has 4 friends



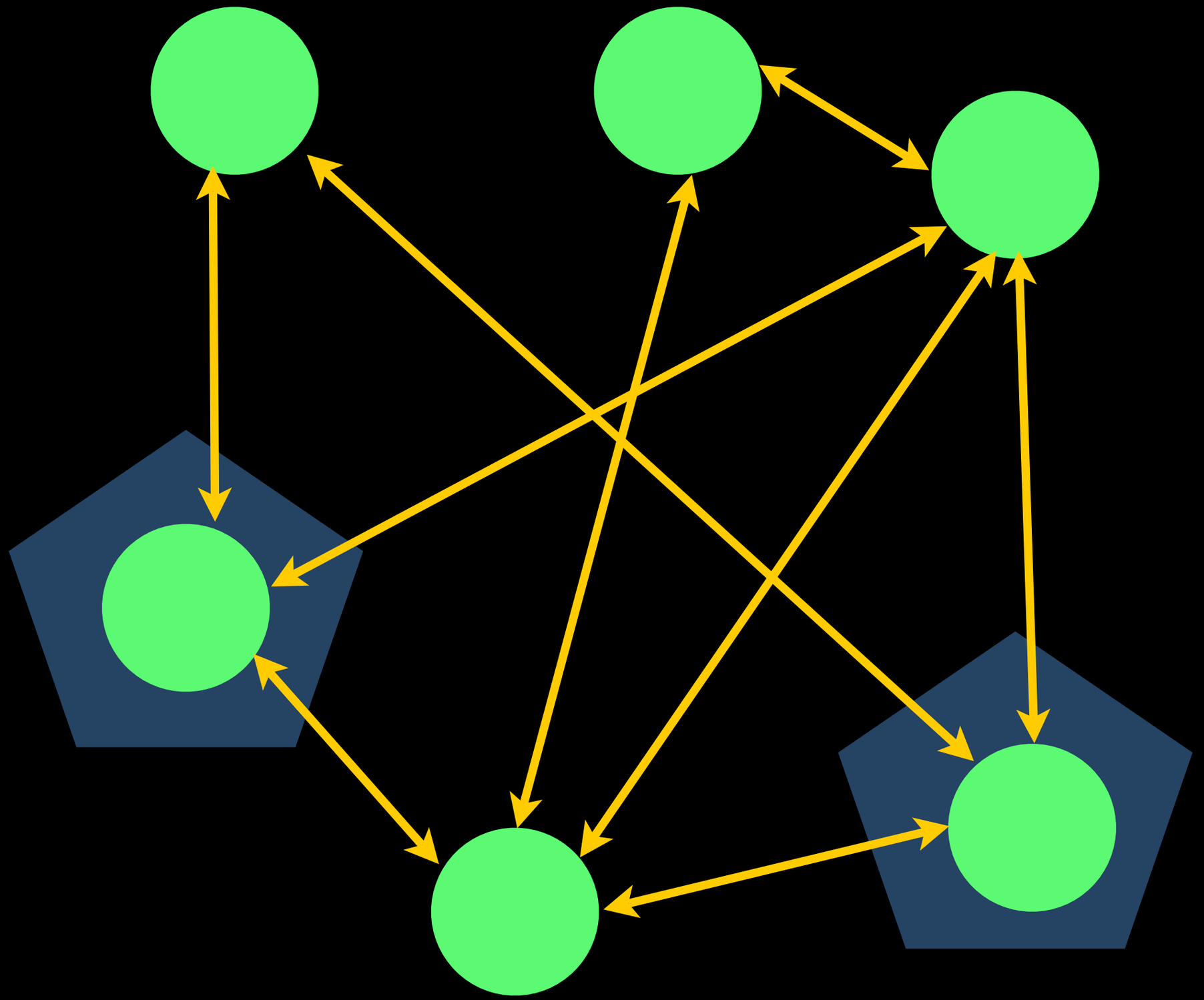
joe has 3 friends, alice has 4 friends



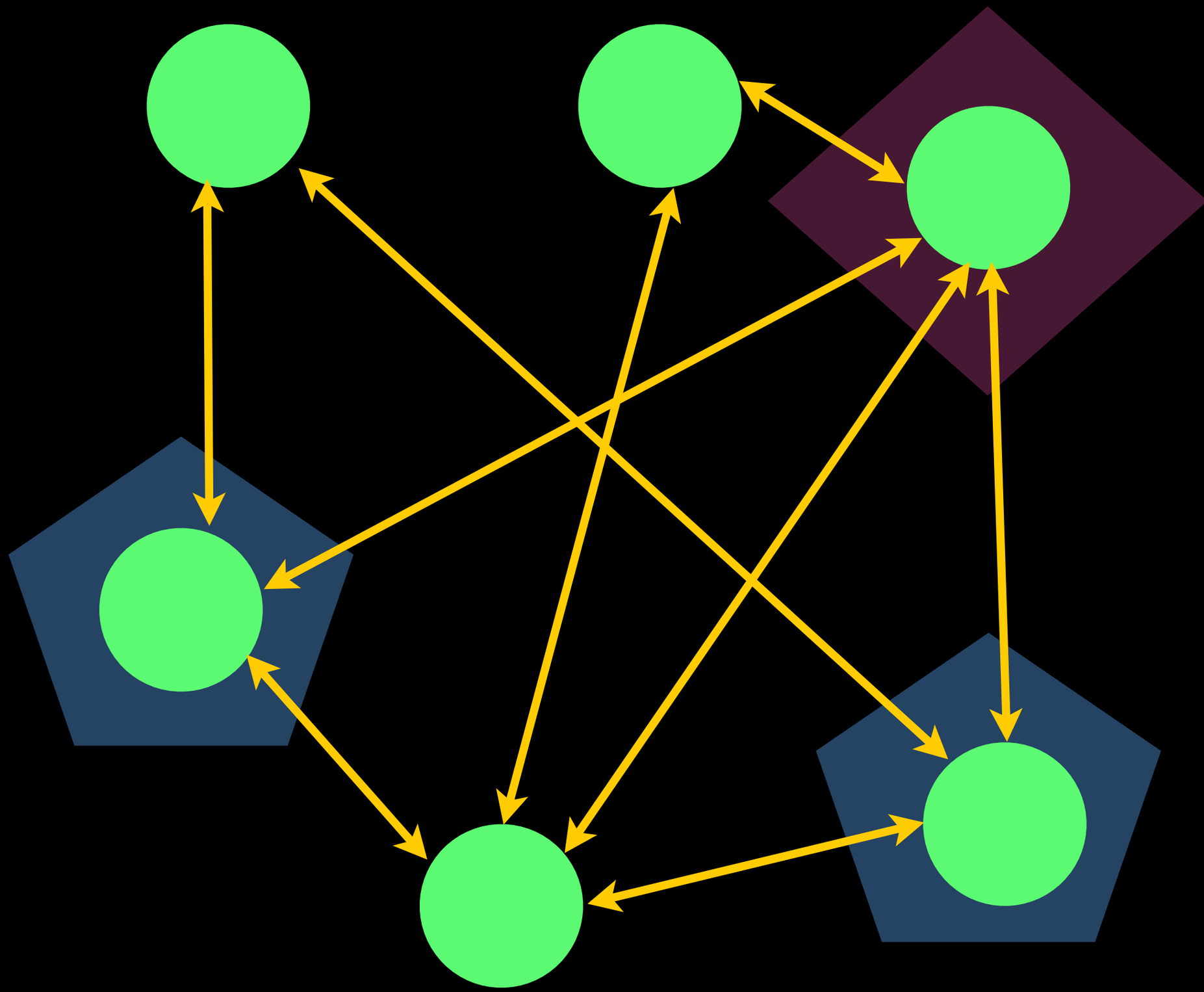
joe has 3 friends, alice has 4 friends



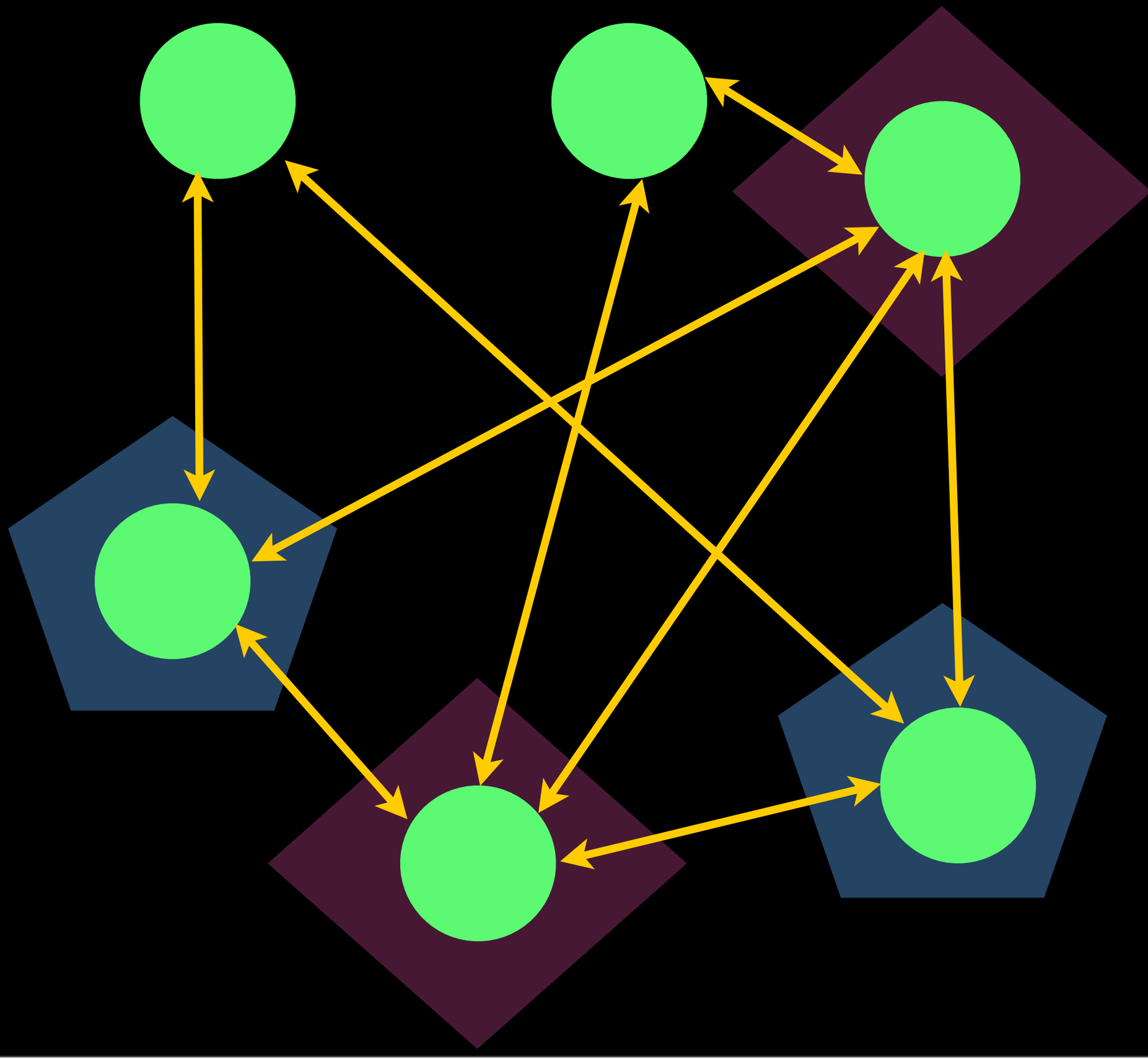
joe has 3 friends, alice has 4 friends



joe has 3 friends, alice has 4 friends



joe has 3 friends, alice has 4 friends



JOE is FRIENDS with ALICE



Facebook fail

- ★ data protection, authn, authz: yes.
- ★ no unlinkability, pseudonymity, unobservability, anonymity
- ★ no privacy in facebook?

FACEBOOK USER UPROAR

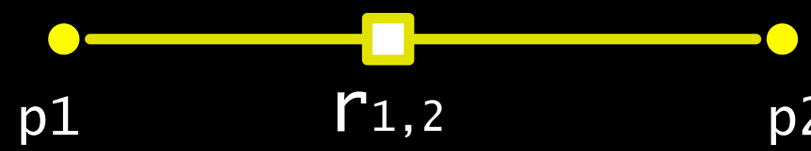
- BEACON: A NEW FEATURE
  - AGGREGATES ACTIVITIES ACROSS SITES
- USERS NOTICED AND ORGANIZED PROTESTS
- FACEBOOK BACKED OFF
- SIMILAR REACTION TO CHANGES IN TERMS OF USE

PRIVACY CONCERNS IN FACEBOOK

- BLOGOSPHERE AND NEWS STATE CONCERNS:
  - INDETERMINATE VISIBILITY
  - LACK OF SEPARATION OF IDENTITIES
  - OWNERSHIP
  - MISAPPROPRIATION

INDETERMINATE VISIBILITY

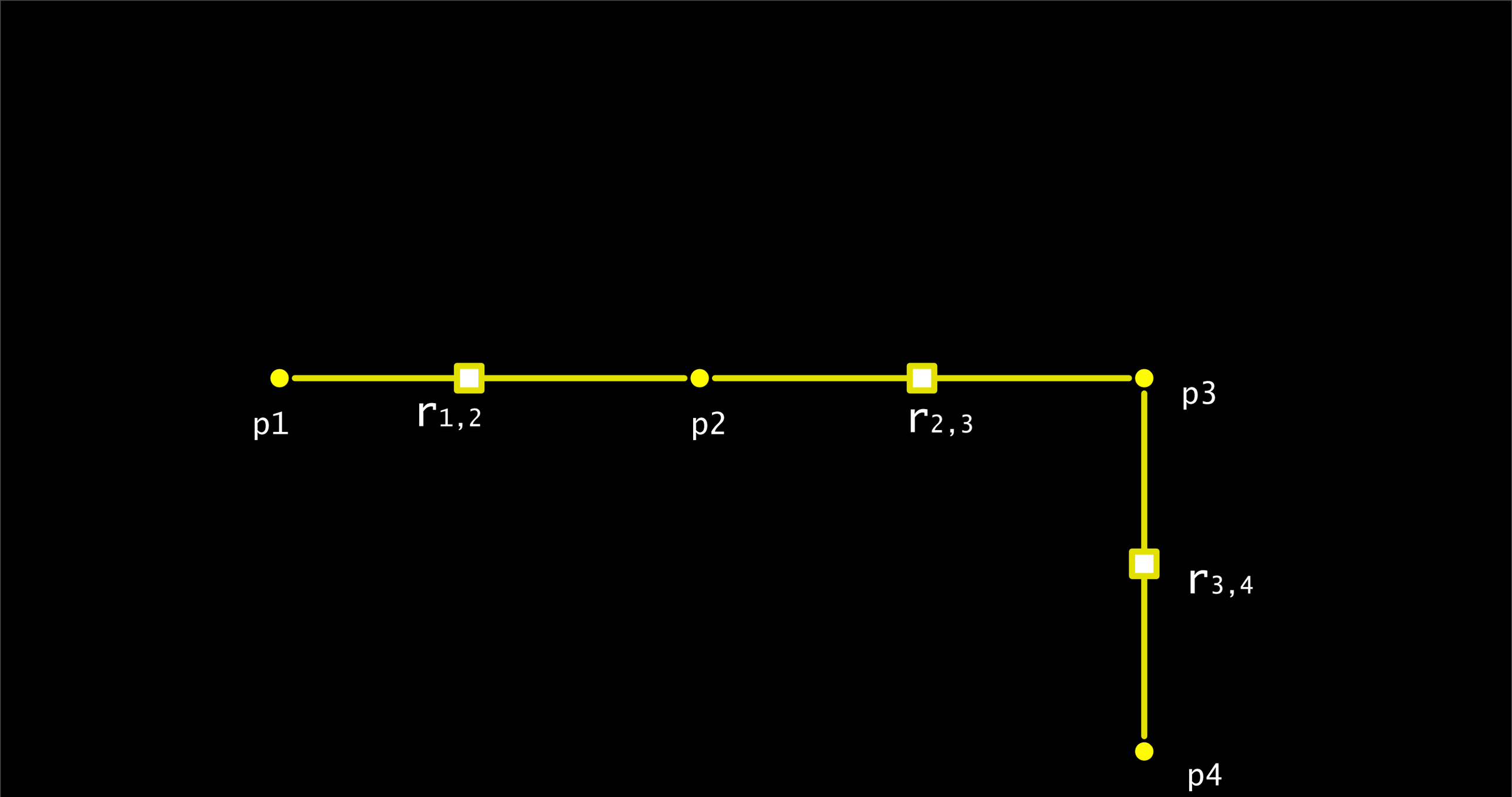
- ★ DATA TRAVELS EASILY
  - ✤ FEATURE CHANGES
  - ✤ RELATIONAL INFORMATION
    - ◉ COMMENTING AND TAGGING
  - ✤ TRANSITIVE ACCESS CONTROL
  - ✤ VARYING DEGREES OF PRIVACY PREFERENCES

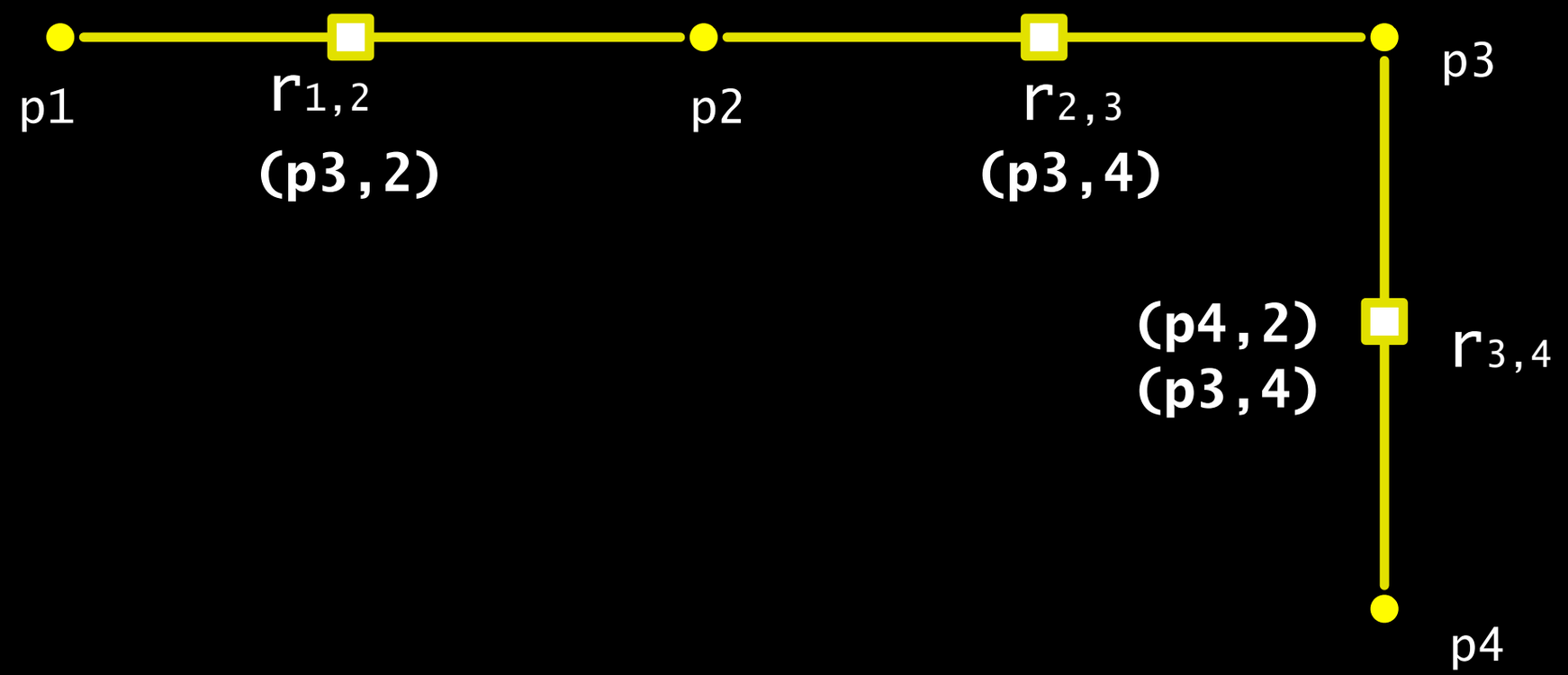

p1
r1,2
p2



(p1, 2)

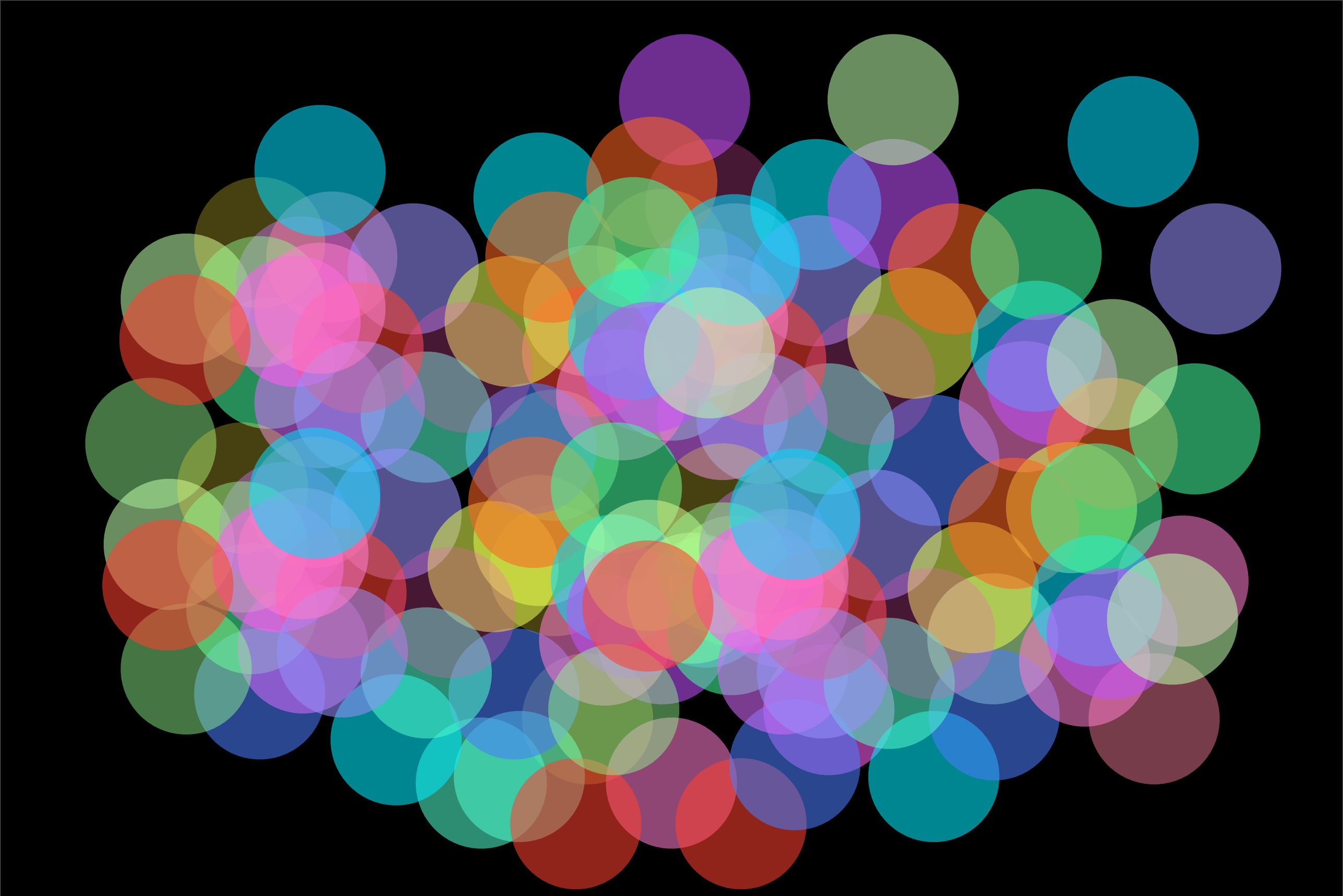
(p2, 2)


p1
$r_{1,2}$
p2
$r_{2,3}$
p3
$r_{3,4}$
p4

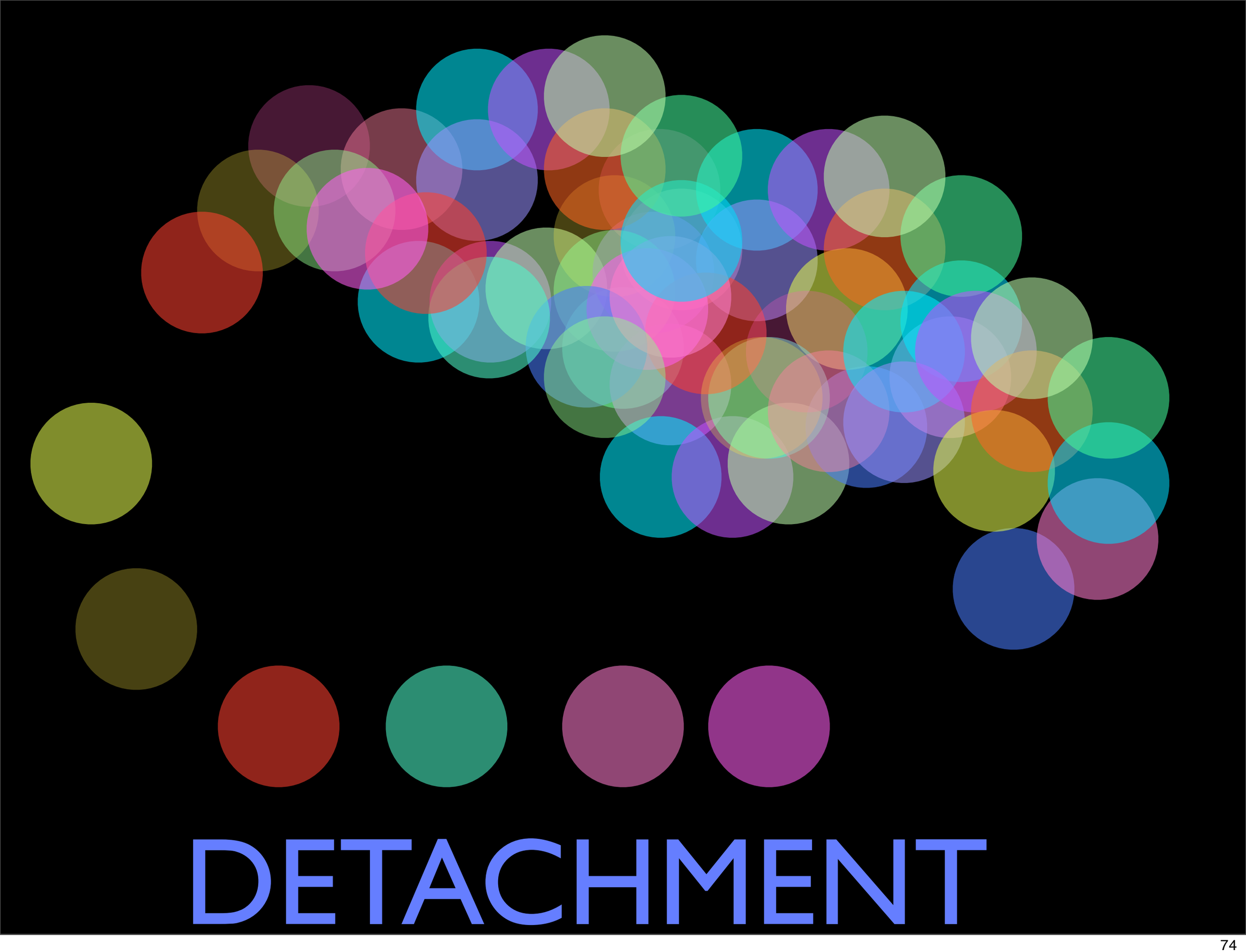

p1
$r_{1,2}$
(p3,2)
p2
$r_{2,3}$
(p3,4)
p3
(p4,2)
(p3,4)
$r_{3,4}$
p4



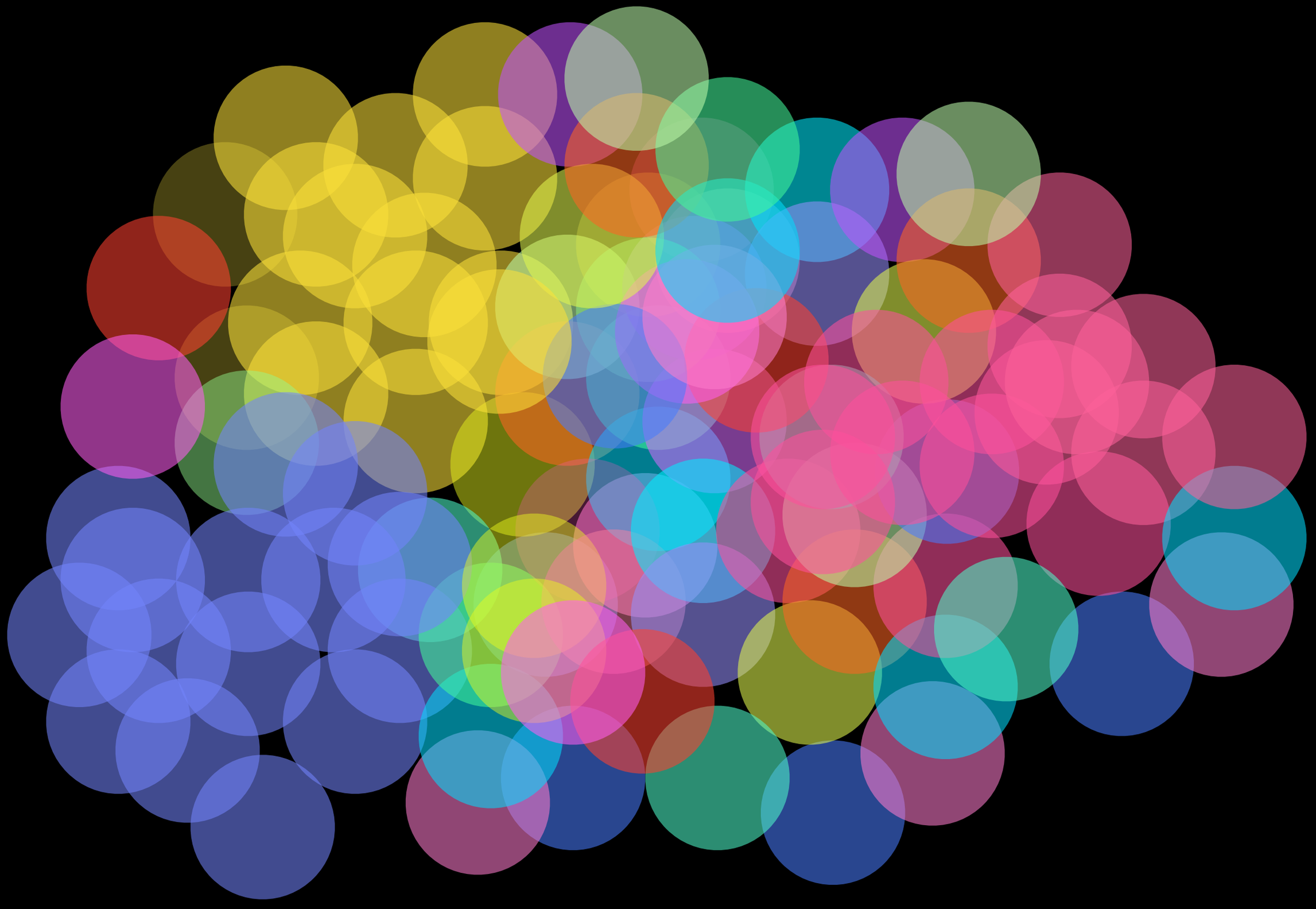
PRIVATE INDIVIDUALS



COLLECTIVES


DETACHMENT

STRATEGIC REVELATION



COLLECTIVE MECHANISMS?

References

- Guarda and Zannone, Towards the development of privacy aware systems, Information and Software technology, 2009
- Kalloniatis et al., Addressing privacy requirements in system design: the Pris Method, Requirements Engineering, 2008