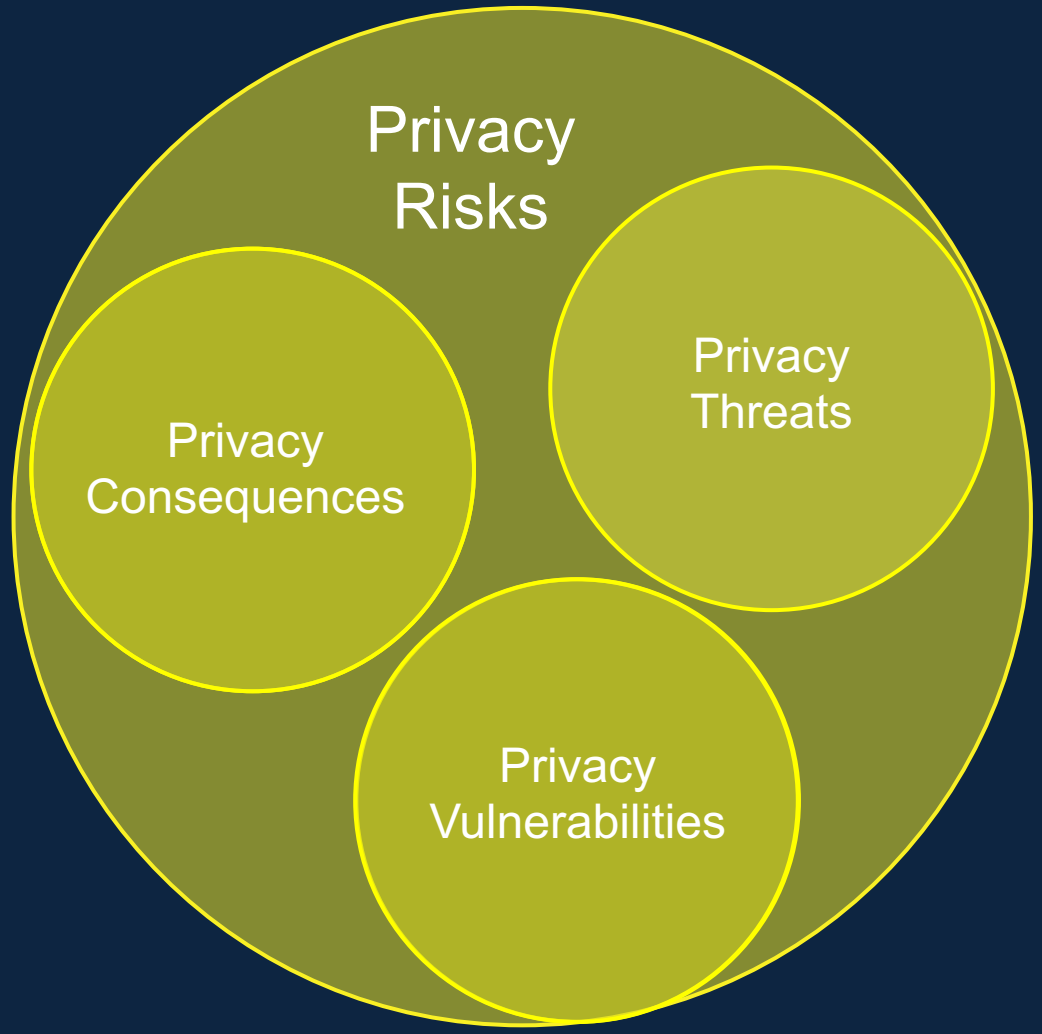
Privacy Threat Modeling

PEPR, June 2022

Cara Bloom

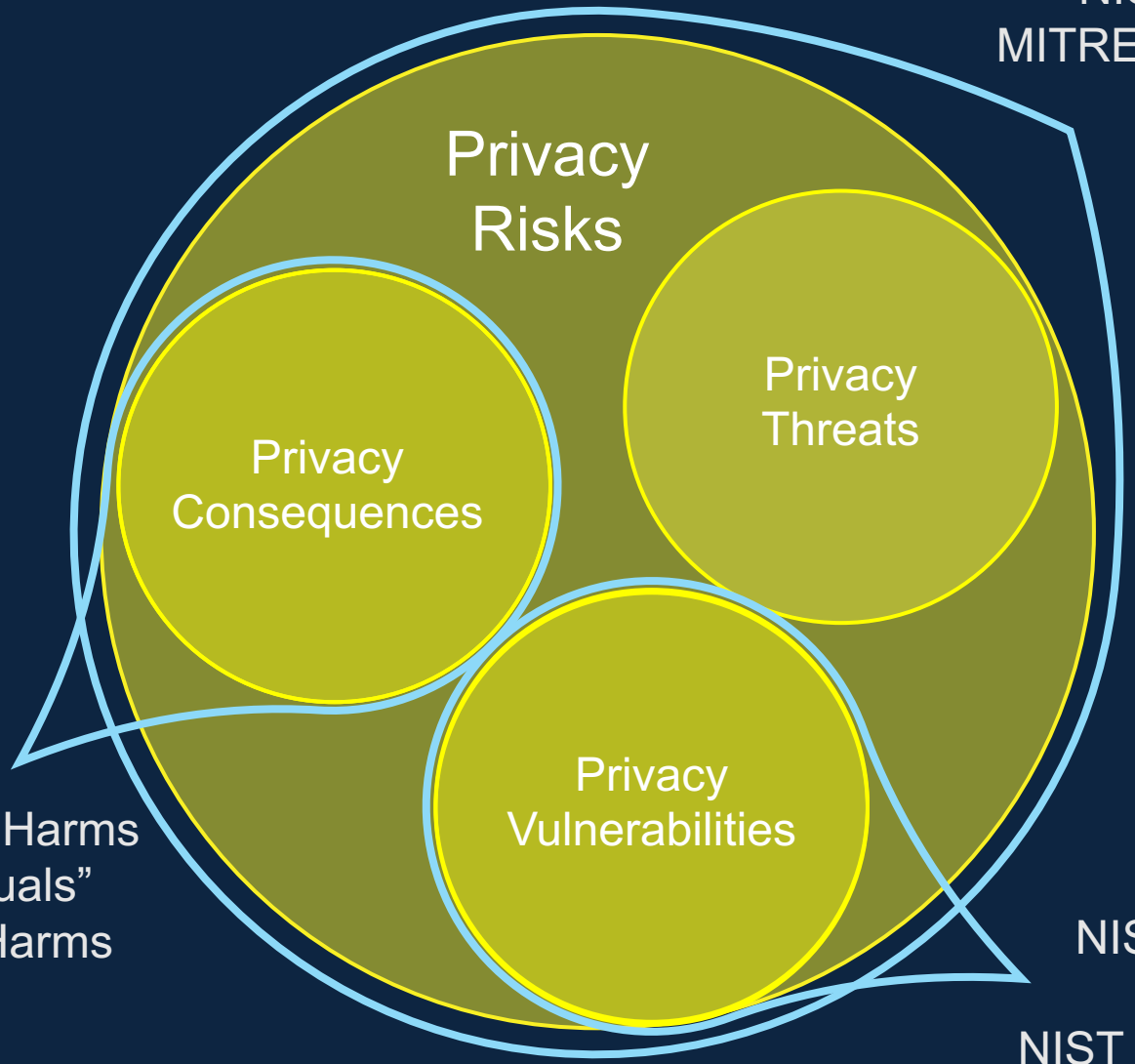
MITRE

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®



MITRE

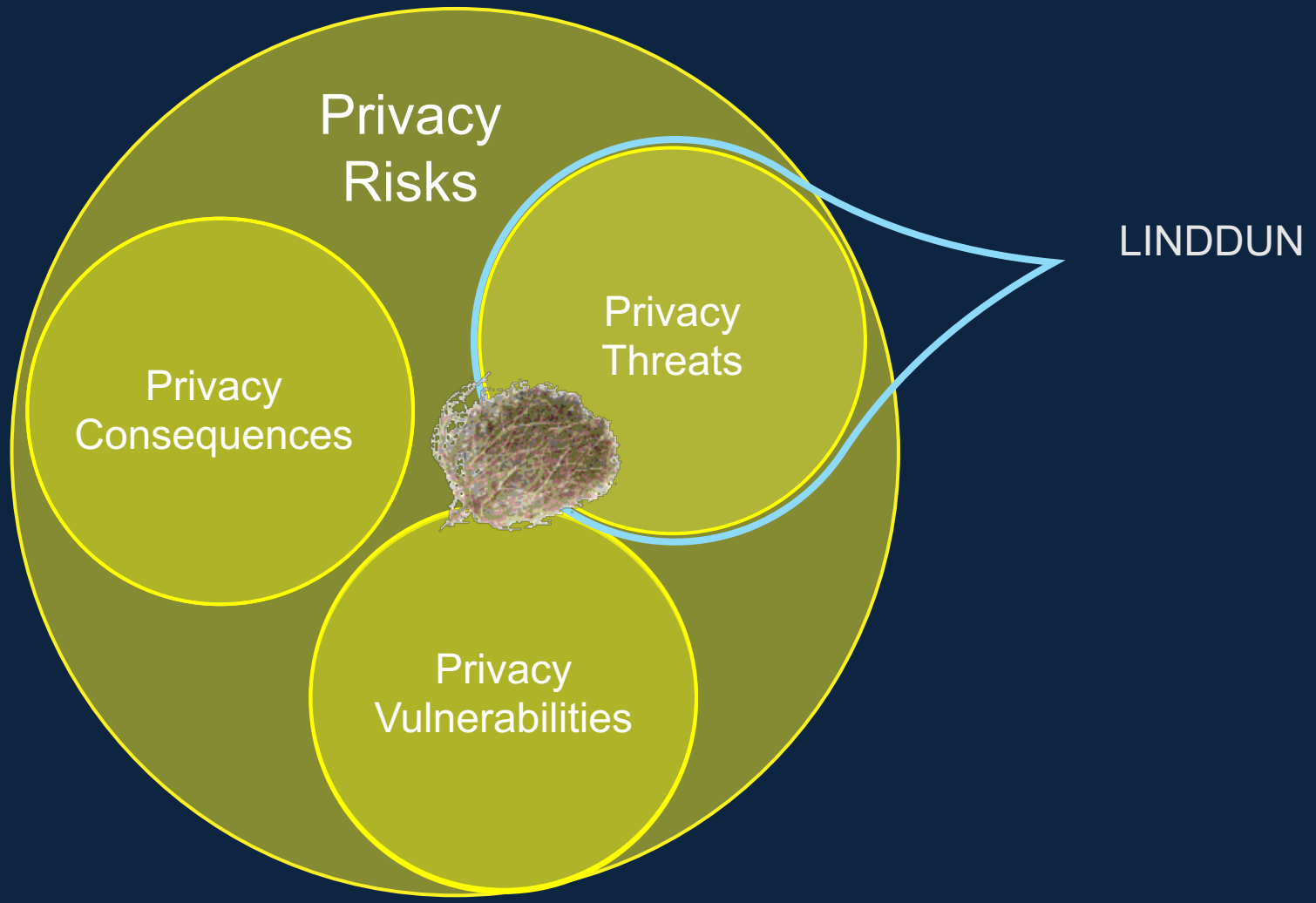
NIST Privacy Risk Assessment Methodology
NIST Privacy Framework
MITRE Privacy Engineering Tools
FAIR-P



Solove's Taxonomy of Privacy Harms
NIST's "problems for individuals"
Calo's Objective/Subjective Harms

NIST SP 800-53 Controls
LINDDUN
NIST Problematic Data Actions
Vulnerability-specific guidance

MITRE

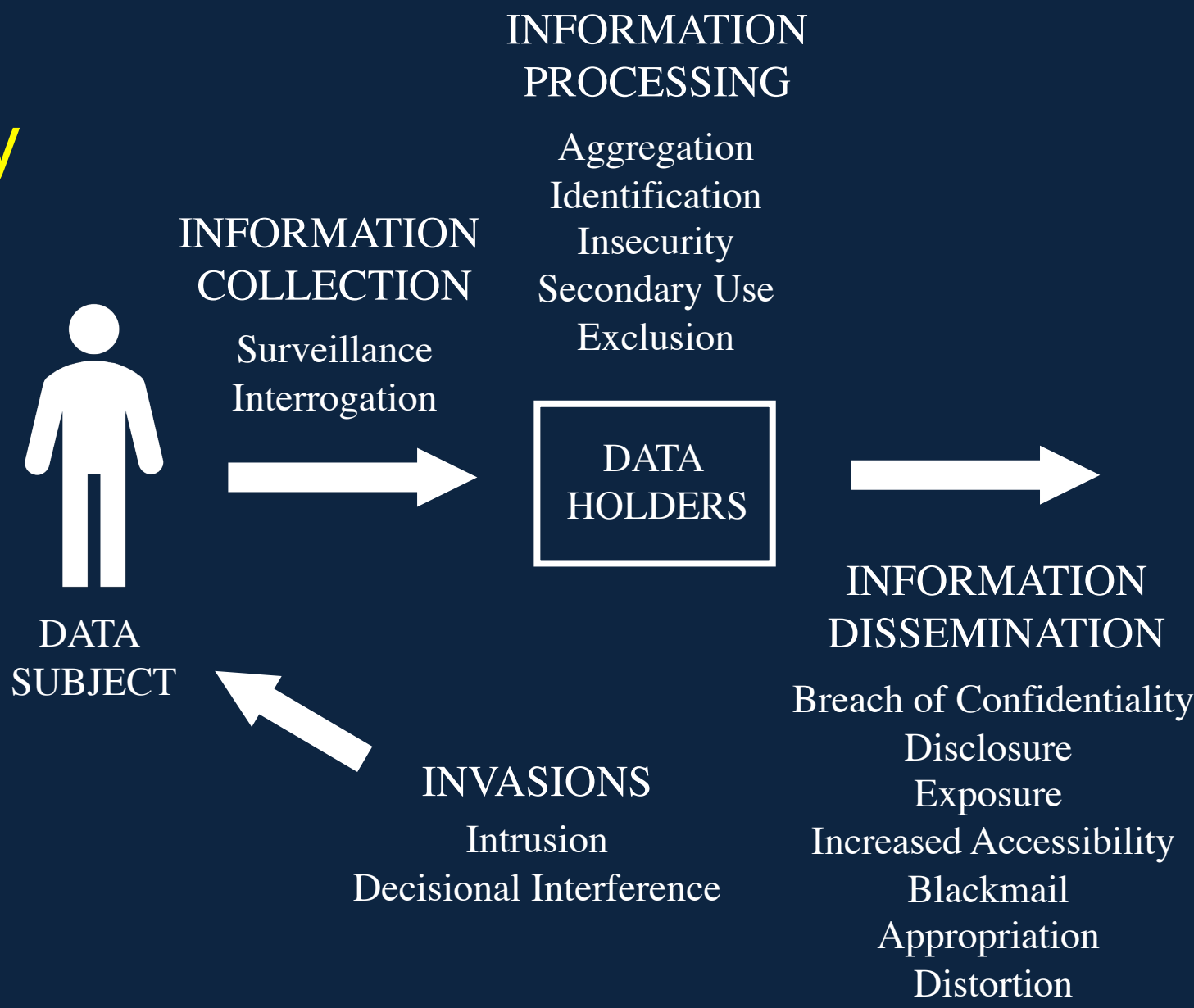


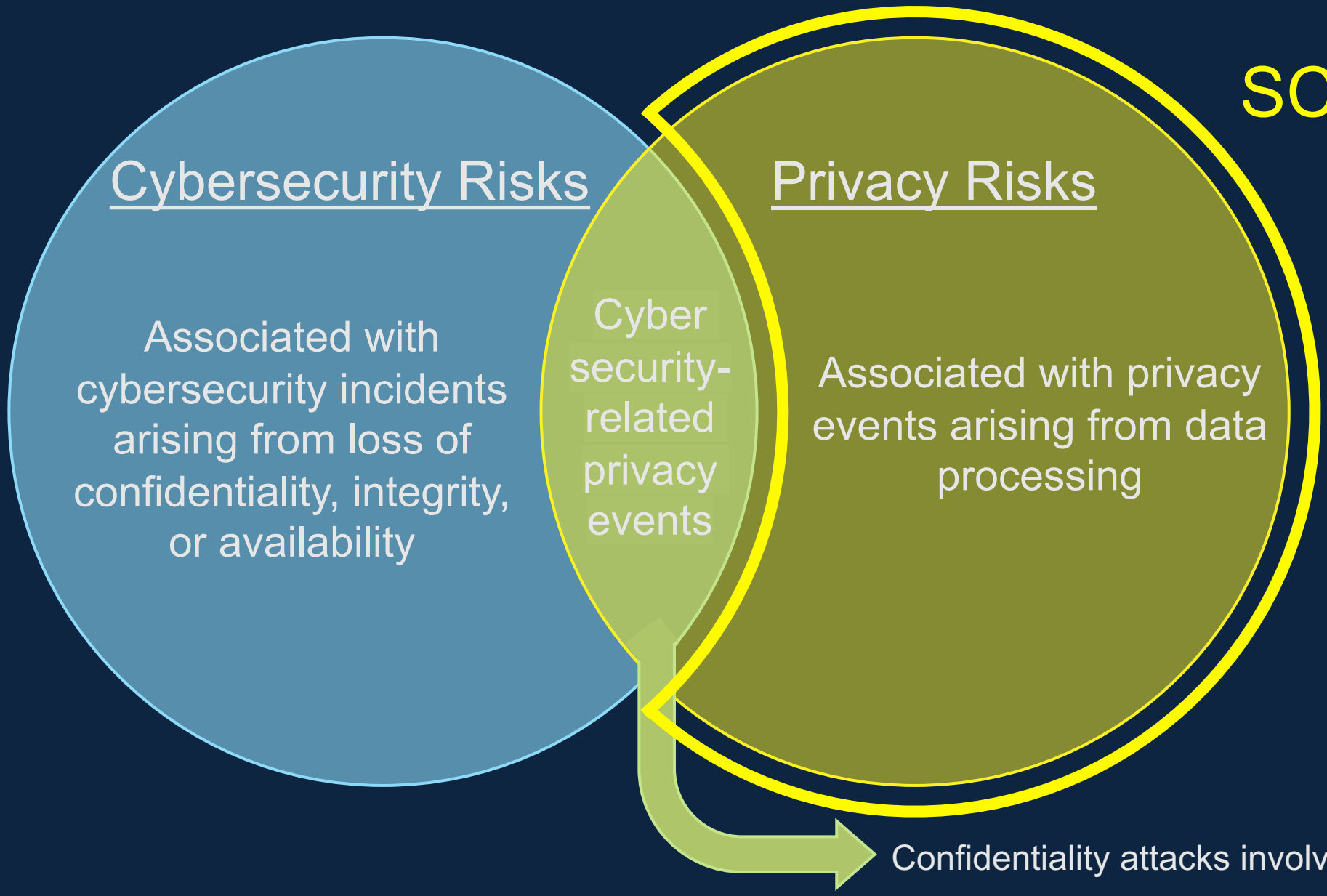
Privacy Attack:

Actions or inactions that cause a perceived privacy harm*, that do not solely involve cybersecurity violations

*As defined by Solove's Taxonomy

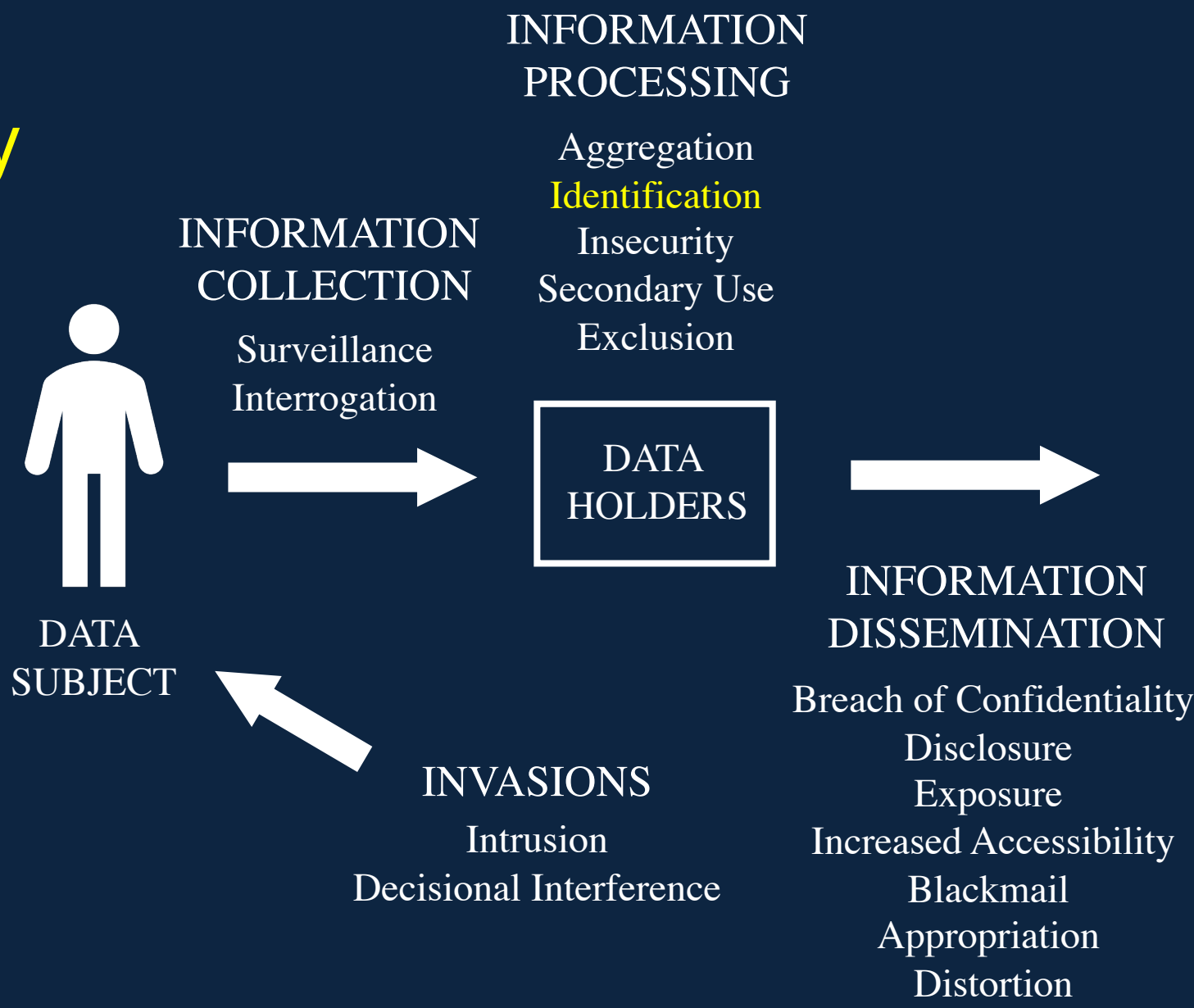
Solove's Taxonomy of Privacy (Harms)





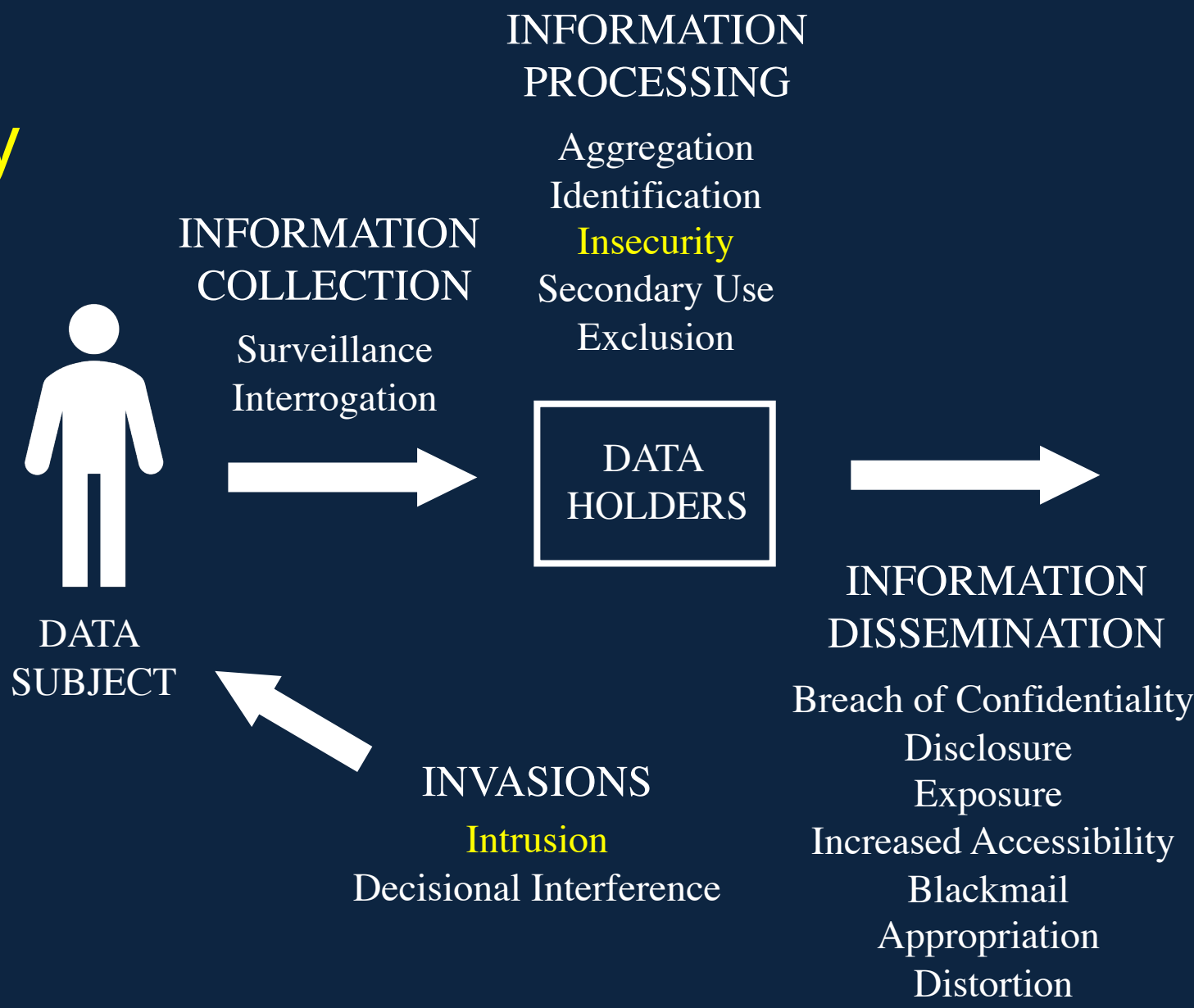
Washington Health Identification

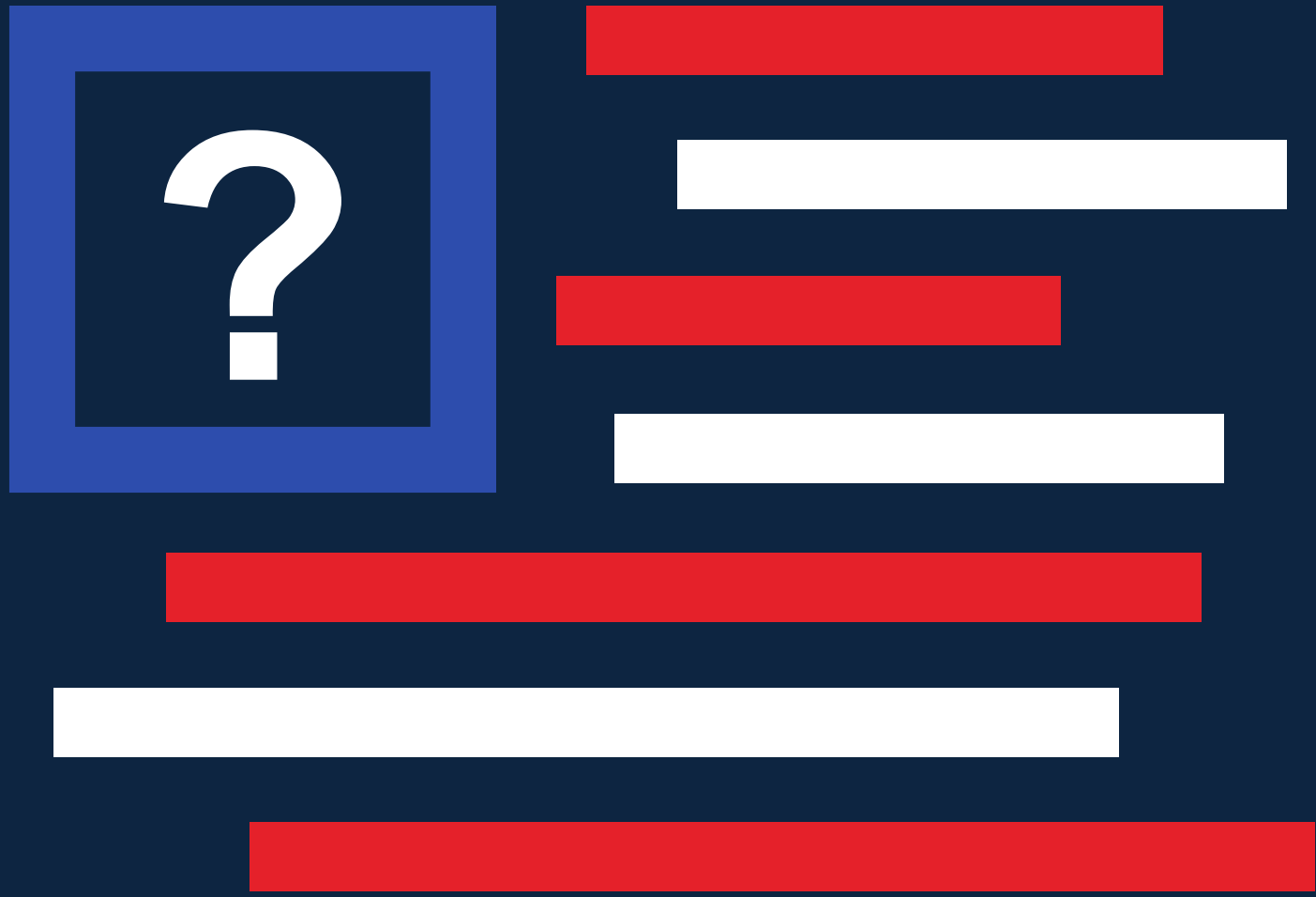
Solove's Taxonomy of Privacy (Harms)



Lenovo Superfish
Insecurity & Intrusion

Solove's Taxonomy of Privacy (Harms)

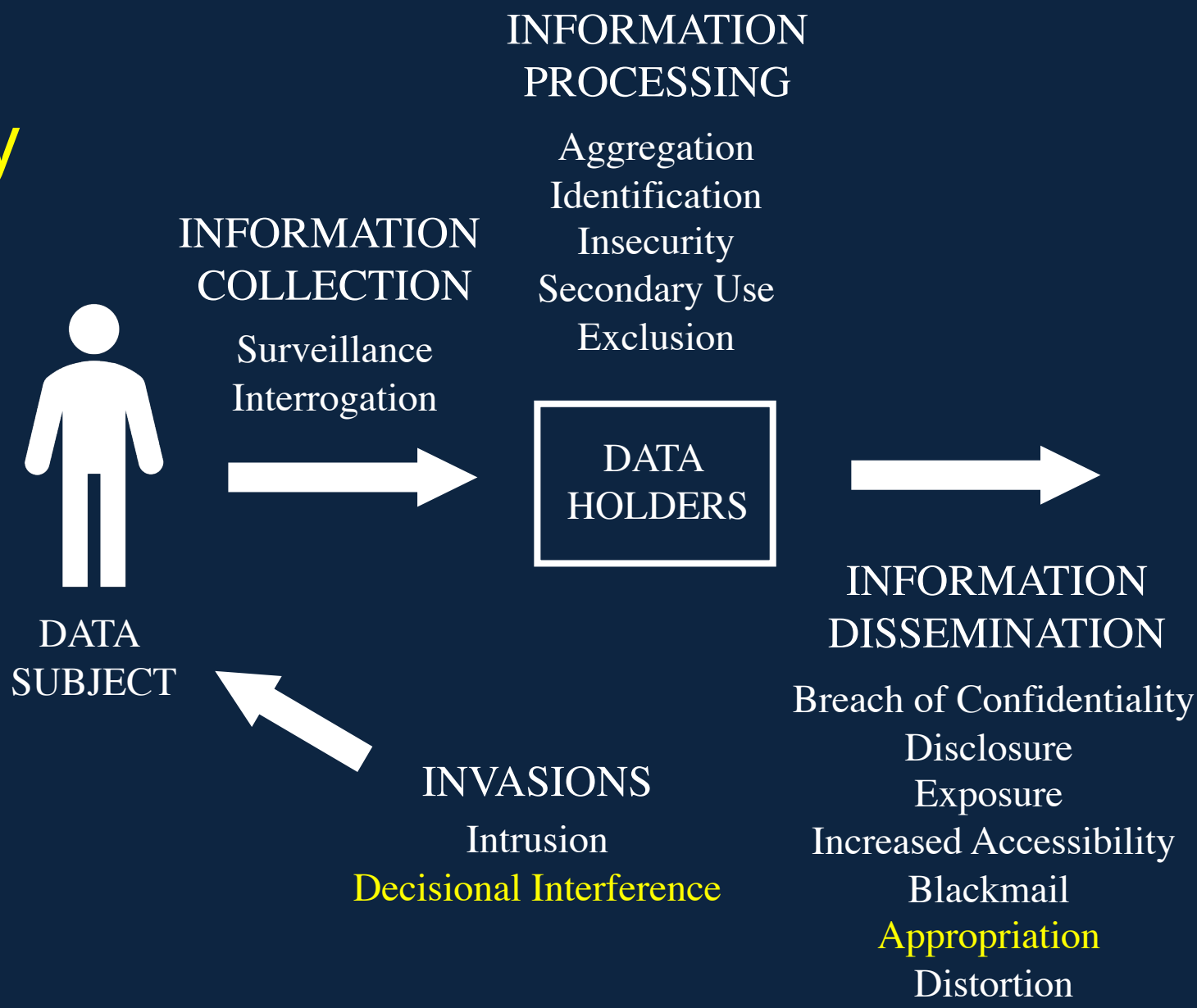


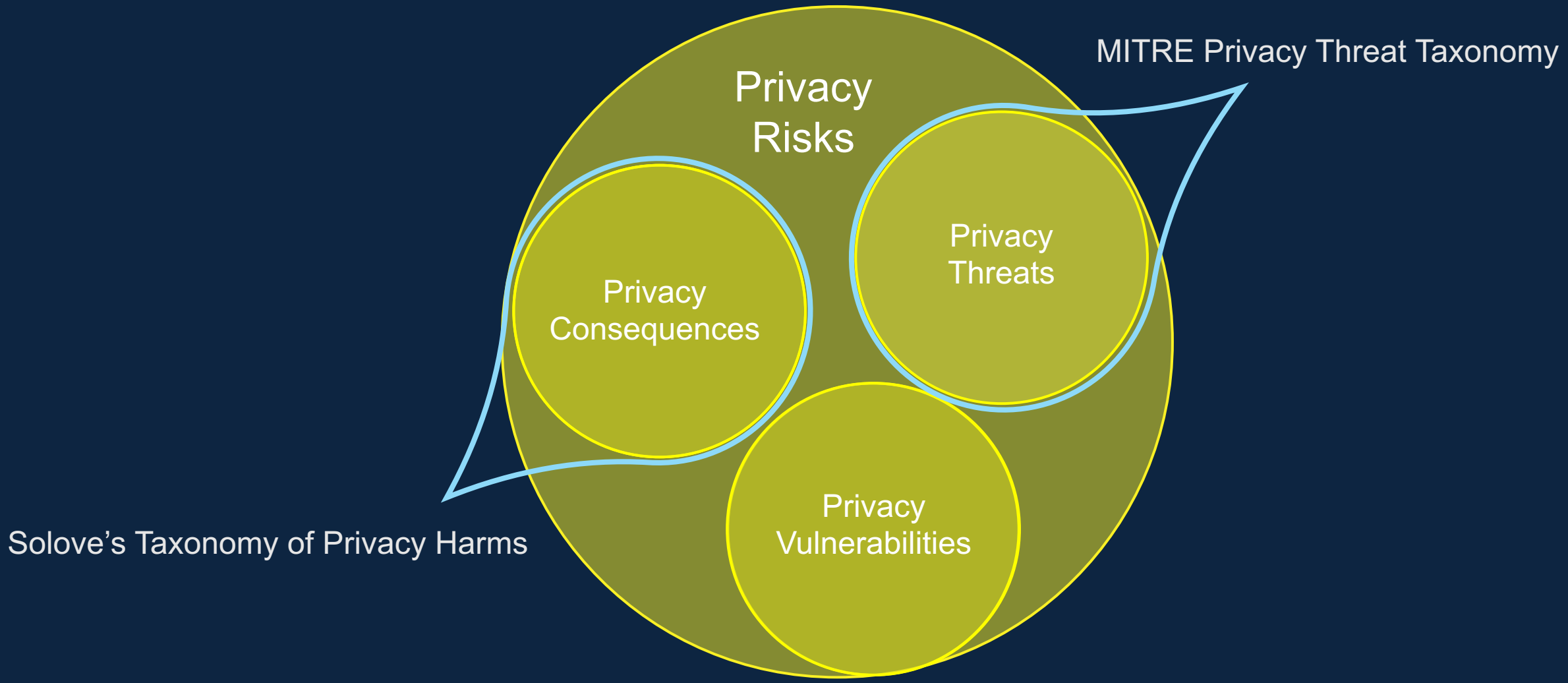


Cambridge Analytica
Appropriation & Decisional Interference

MITRE

Solove's Taxonomy of Privacy (Harms)





Privacy risk management is the exception, not the rule

RISK MANAGEMENT

COMPLIANCE

TECHNICAL DEVELOPMENT OF THE

PRIVACY THREAT TAXONOMY

DATASET GENERATION

Applied method from Garfinkel & Theofanos (2018)

- FTC & FCC closed cases involving privacy
- Selected cases that fit our definition of a Privacy Attack

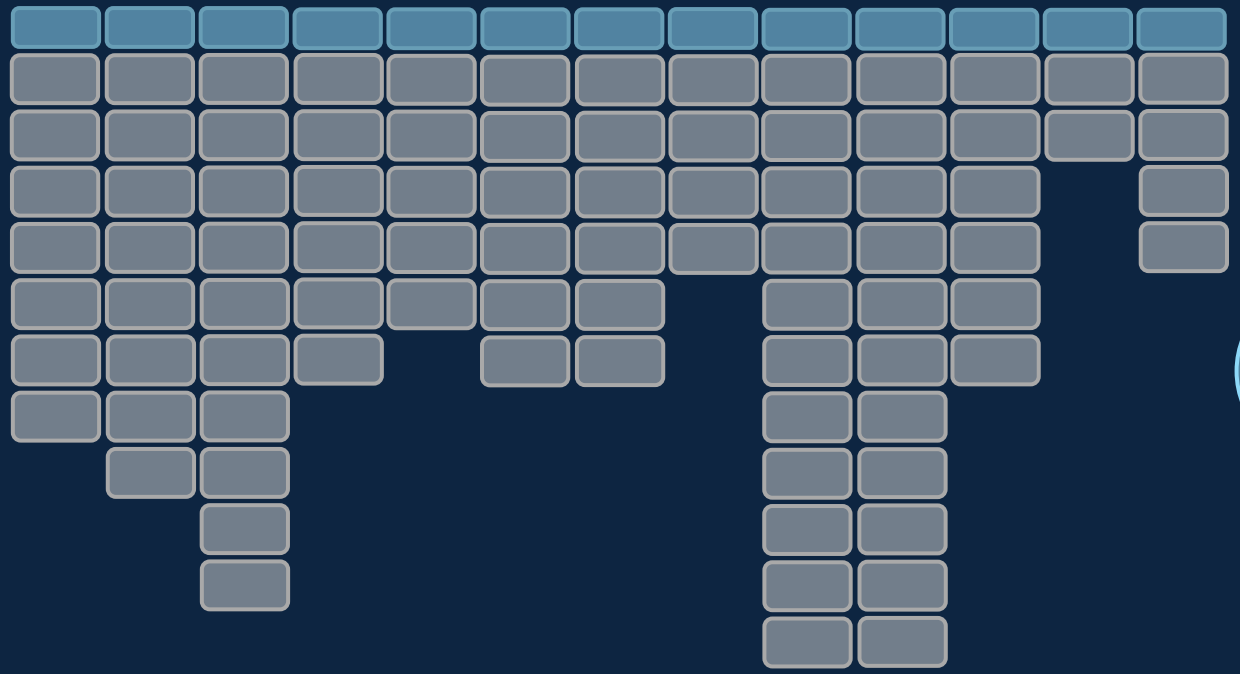
146 Privacy Attacks identified

- Scope: 2000-present
- Catalogued with relevant meta-data

MITRE

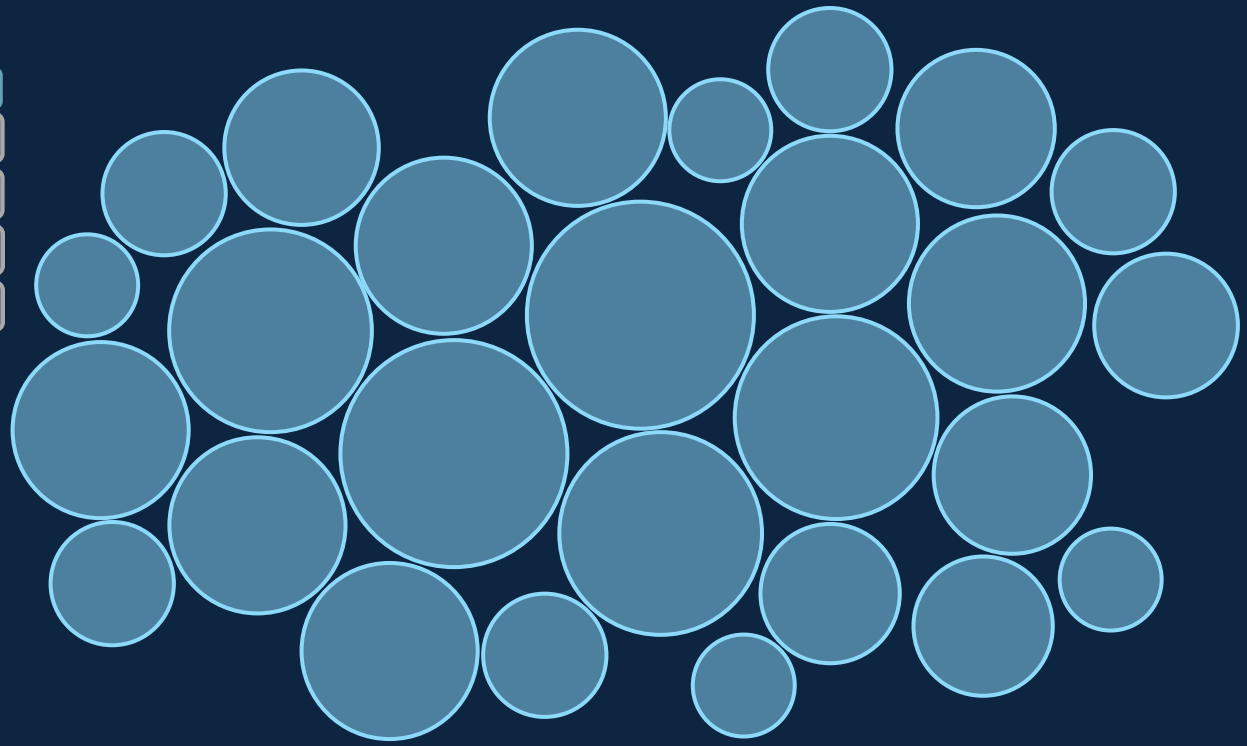
PROTOTYPES

Privacy Threat Taxonomy



Hierarchical ontology of attack components

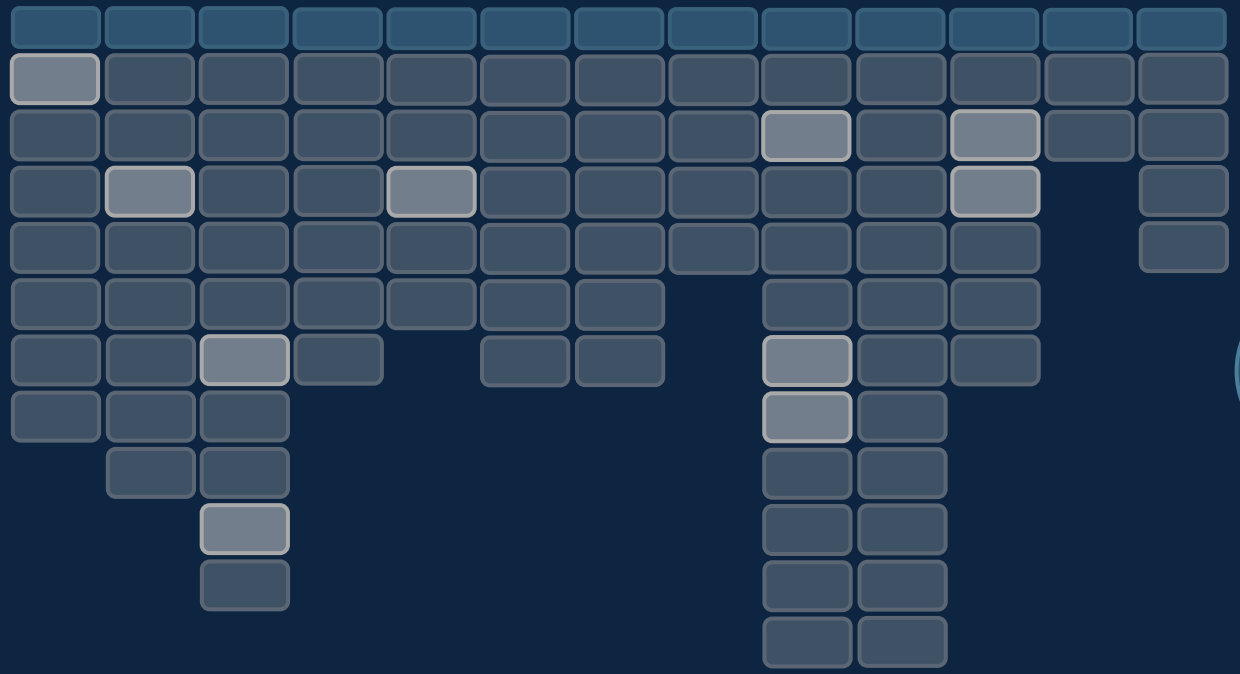
Privacy Threat Clusters



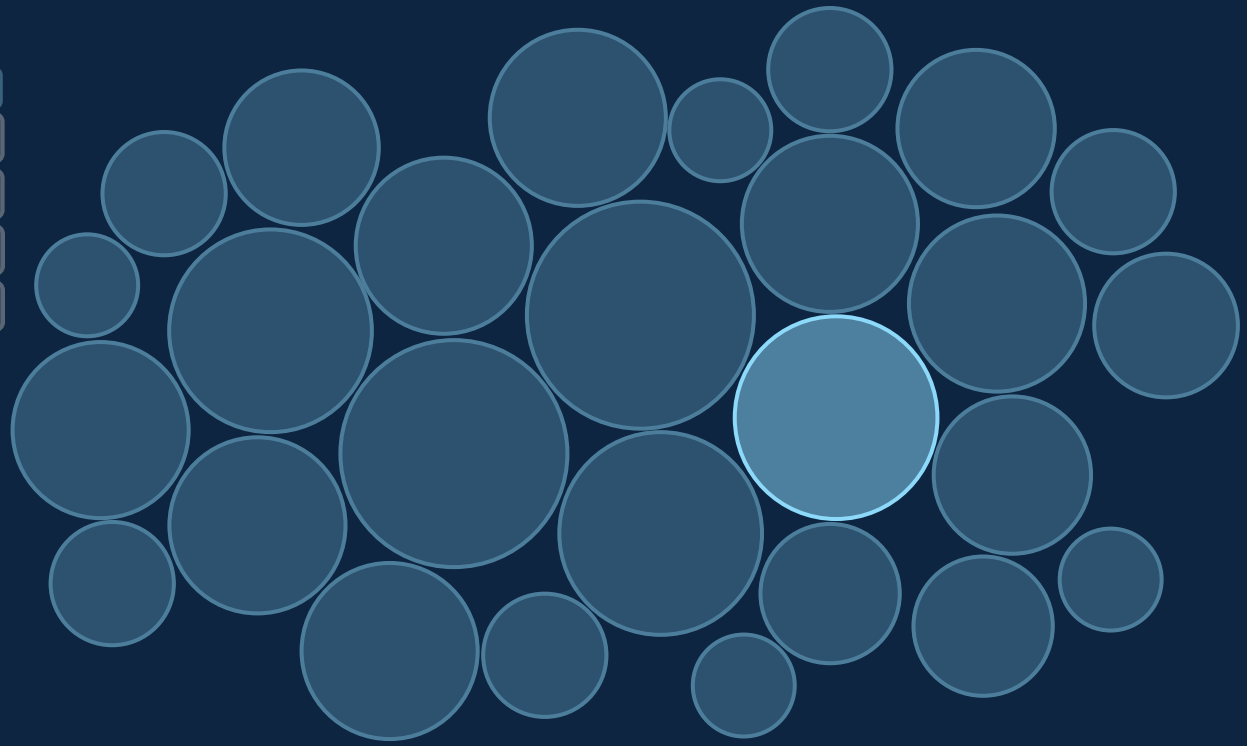
Typology of attacks

PROTOTYPES

Privacy Threat Taxonomy



Privacy Threat Clusters



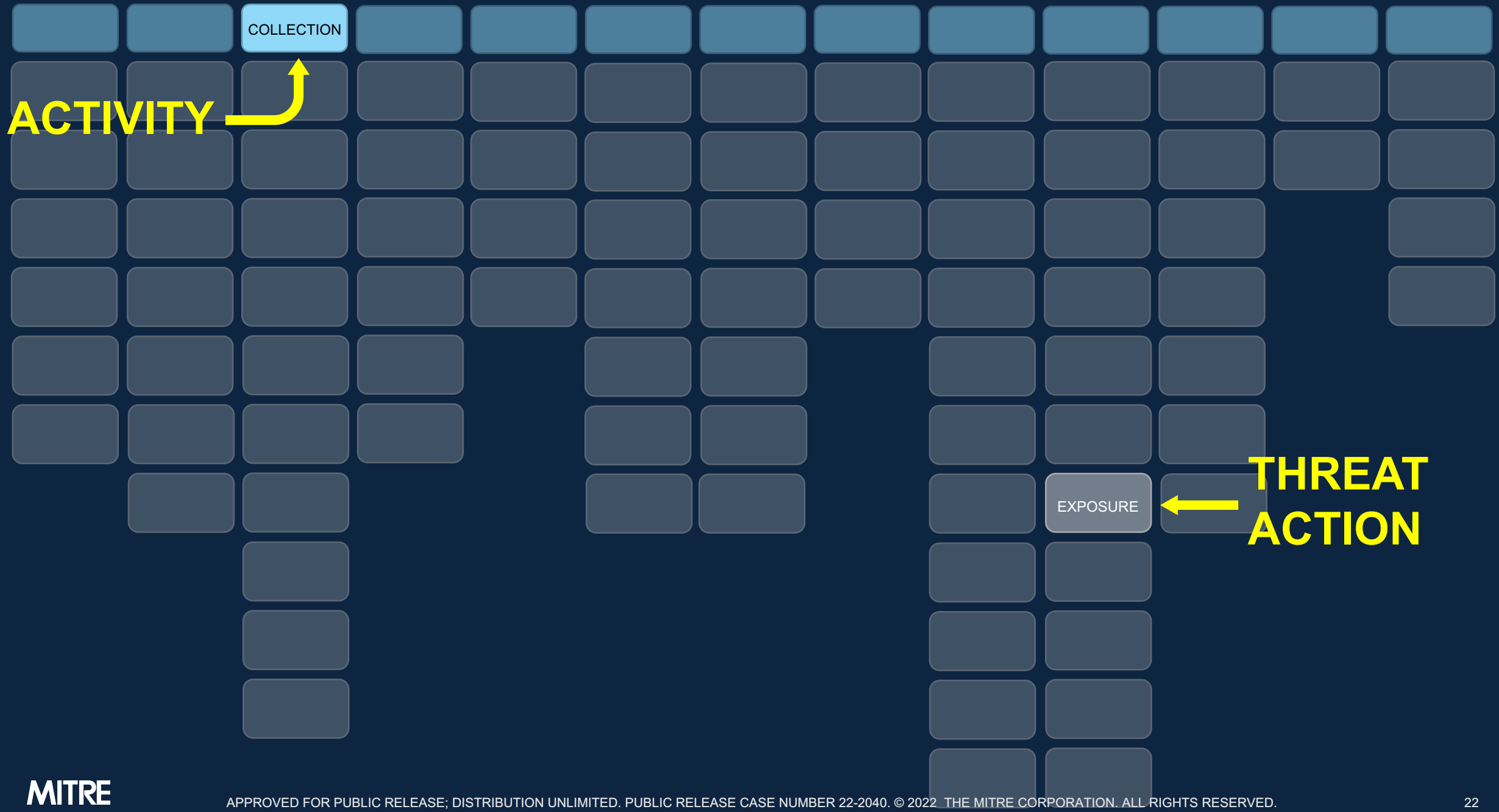
Privacy Threat Pattern Example

STRUCTURING

STRUCTURING

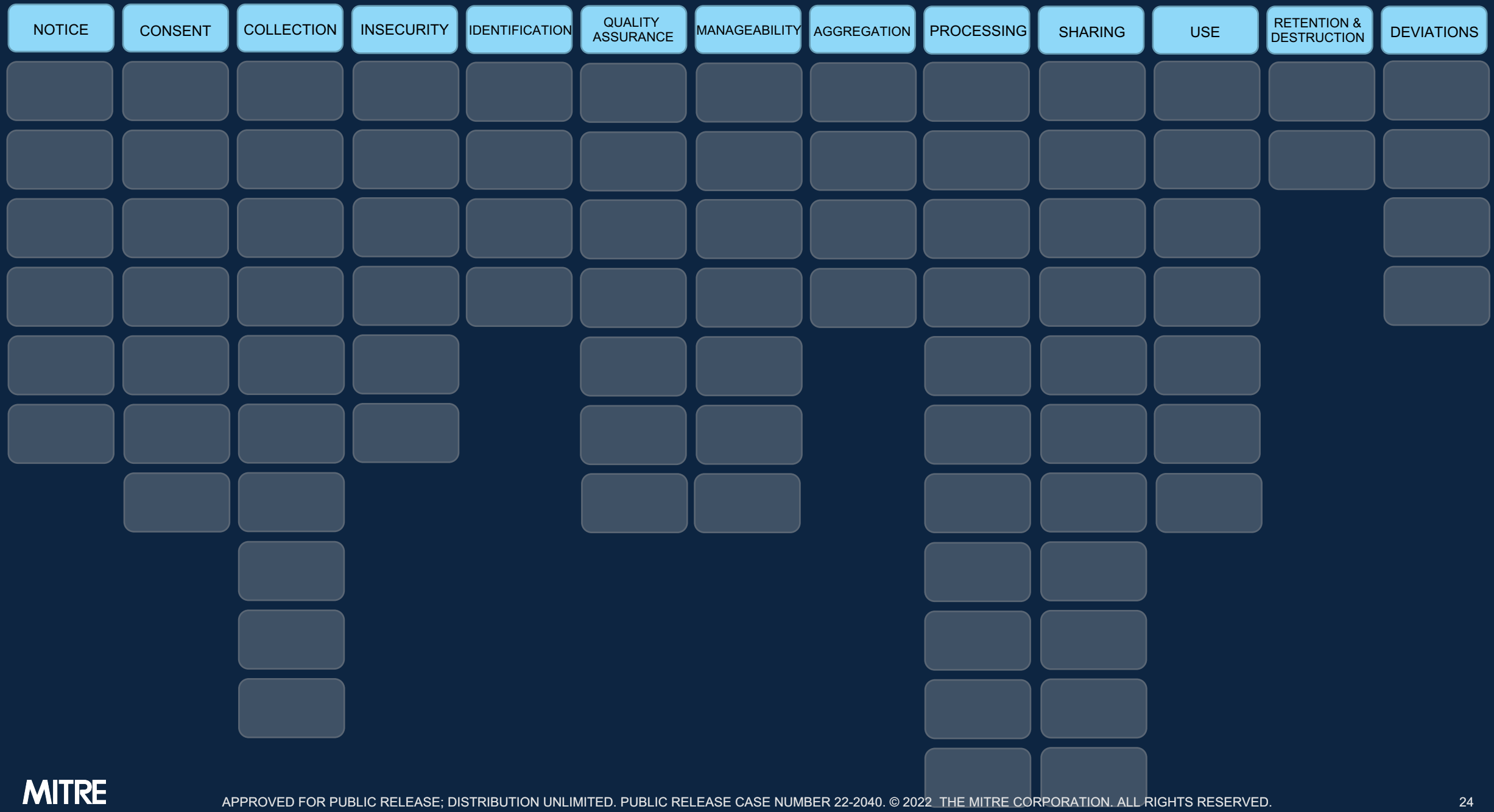
- Break attacks into individual threat actions
- Group threat actions into domains of similar activities

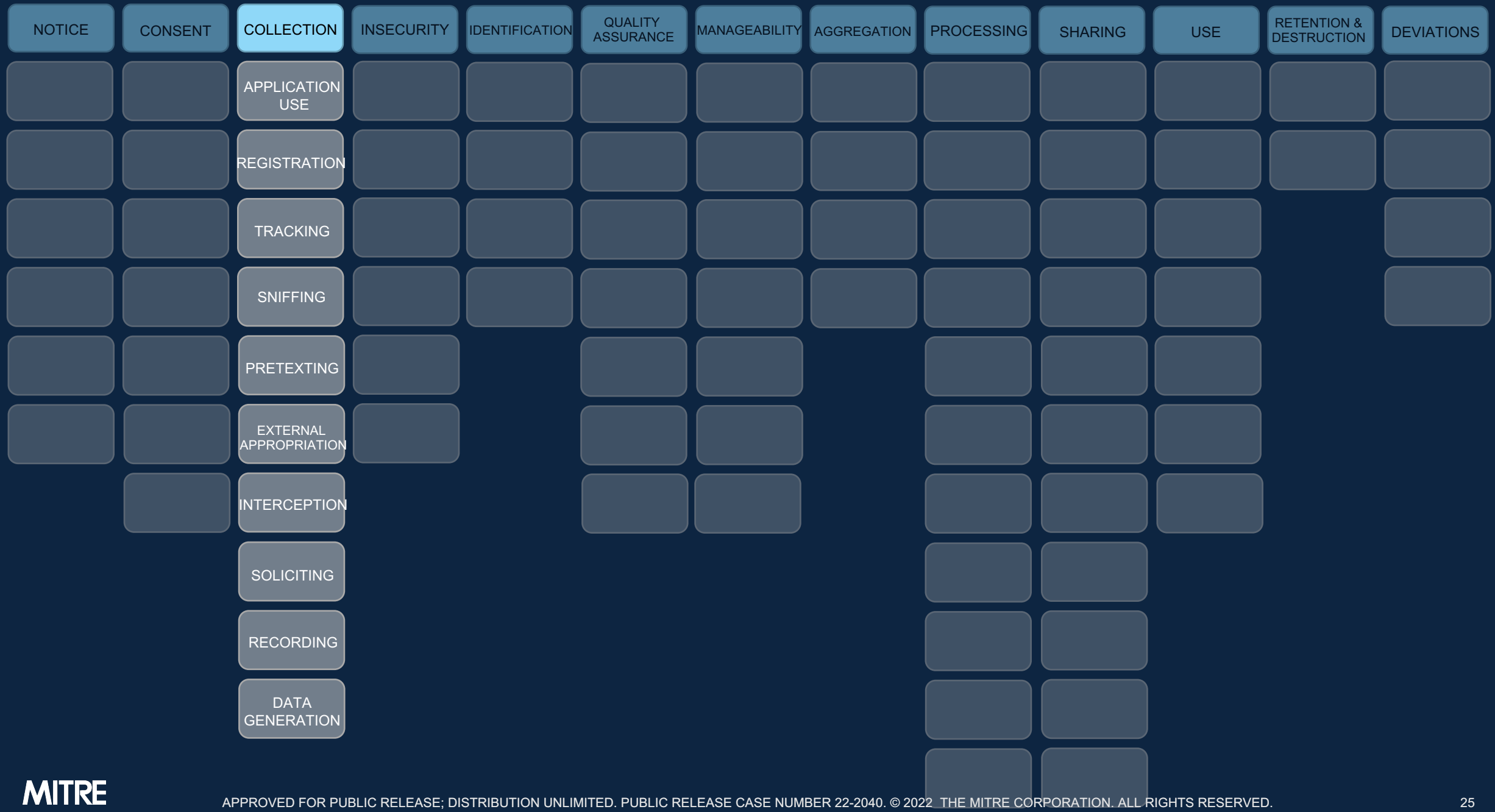
MITRE



STRUCTURING

- Break attacks into individual threat actions
- Group threat actions into domains of similar activities
- Refine threat actions and activities so that there are few overlaps and gaps by mapping individual attacks against the existing taxonomy
- Continue until taxonomy stabilizes

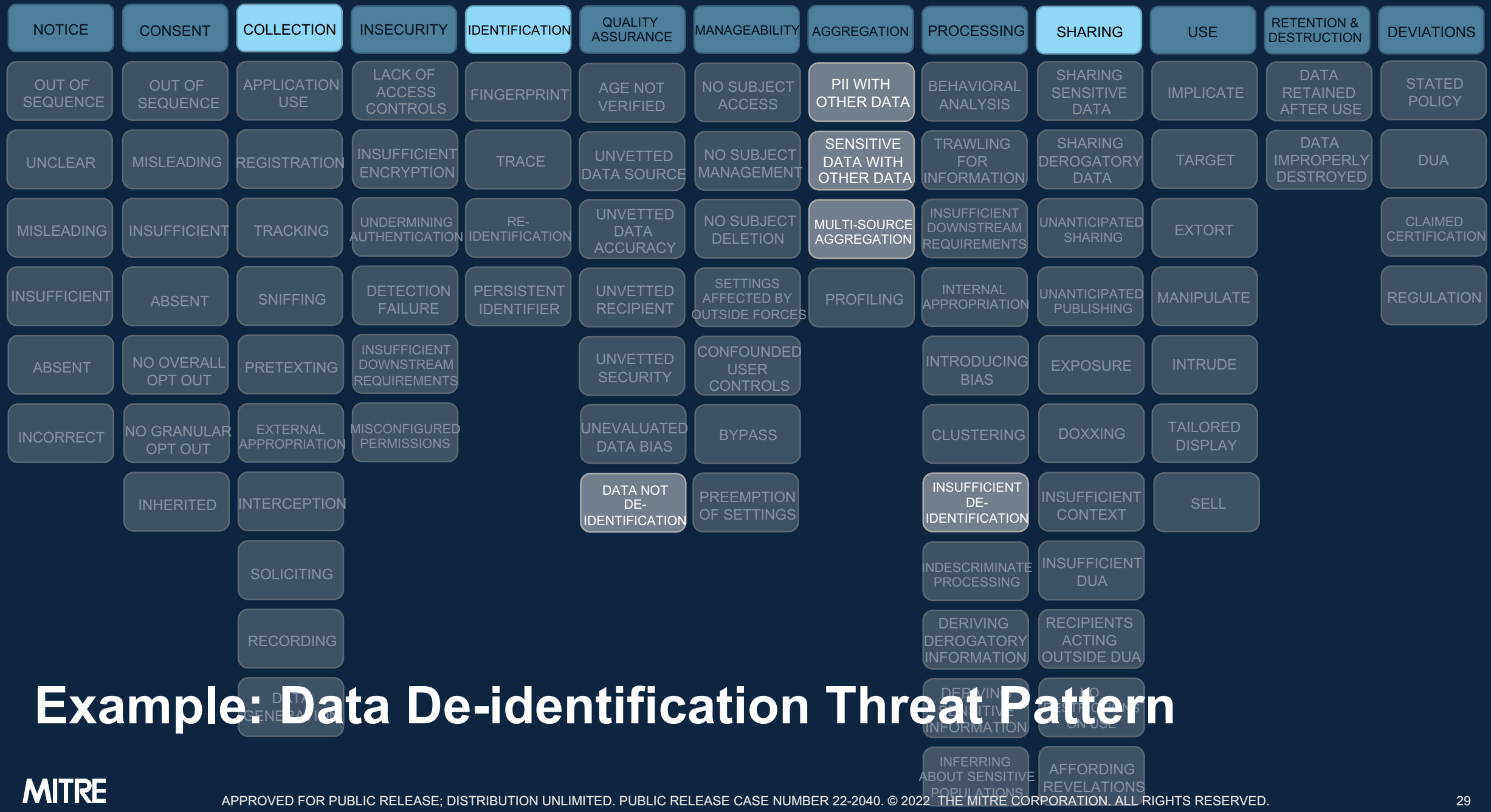




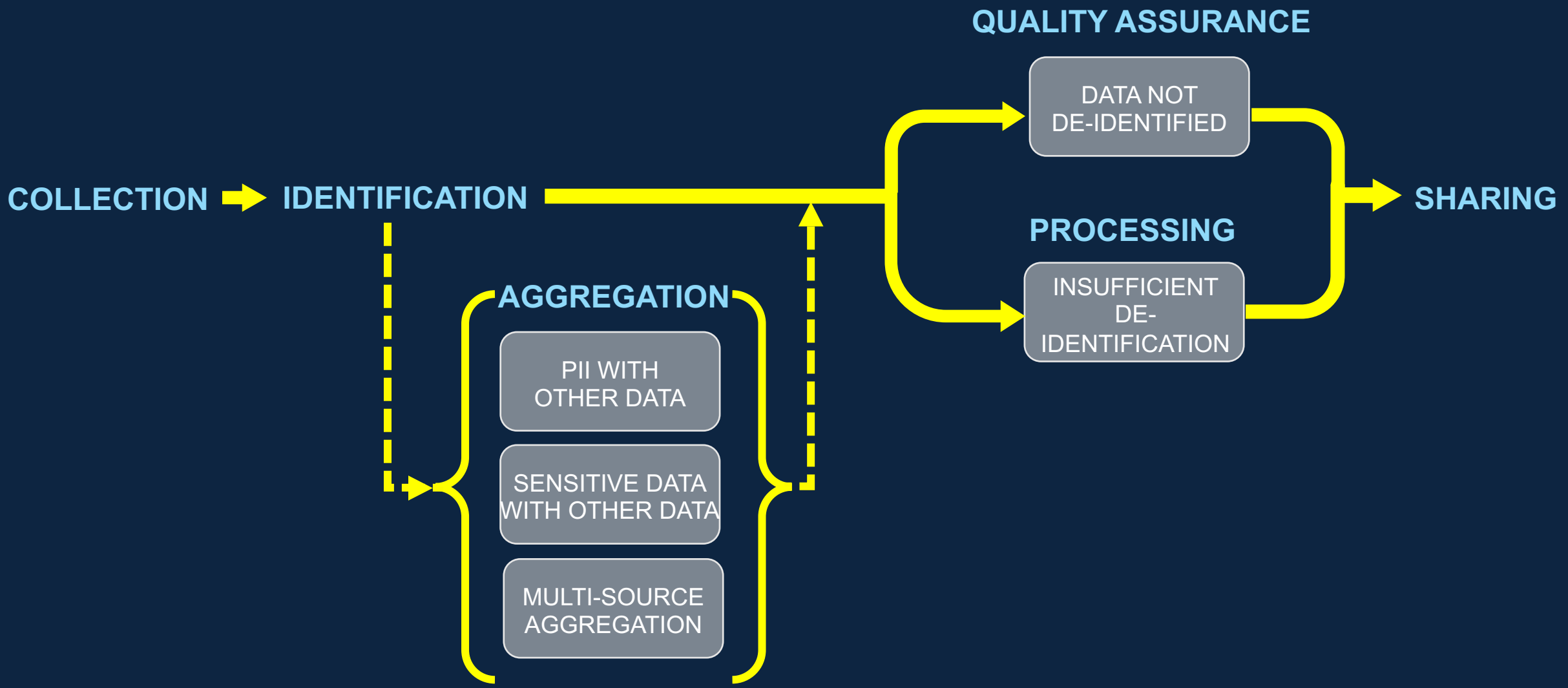
CLUSTERING & THREAT PATTERNS

- Break attacks into individual threat actions
- Cluster attacks with similar threat actions into Threat Clusters
- Map all attacks in dataset to existing groupings, refining and renaming Threat Clusters as needed
- Map each Threat Cluster to the Taxonomy
- Using the threat actions from the taxonomy, assemble a generic killchains for each Cluster, called Threat Patterns

Example: Data De-identification Threat Pattern

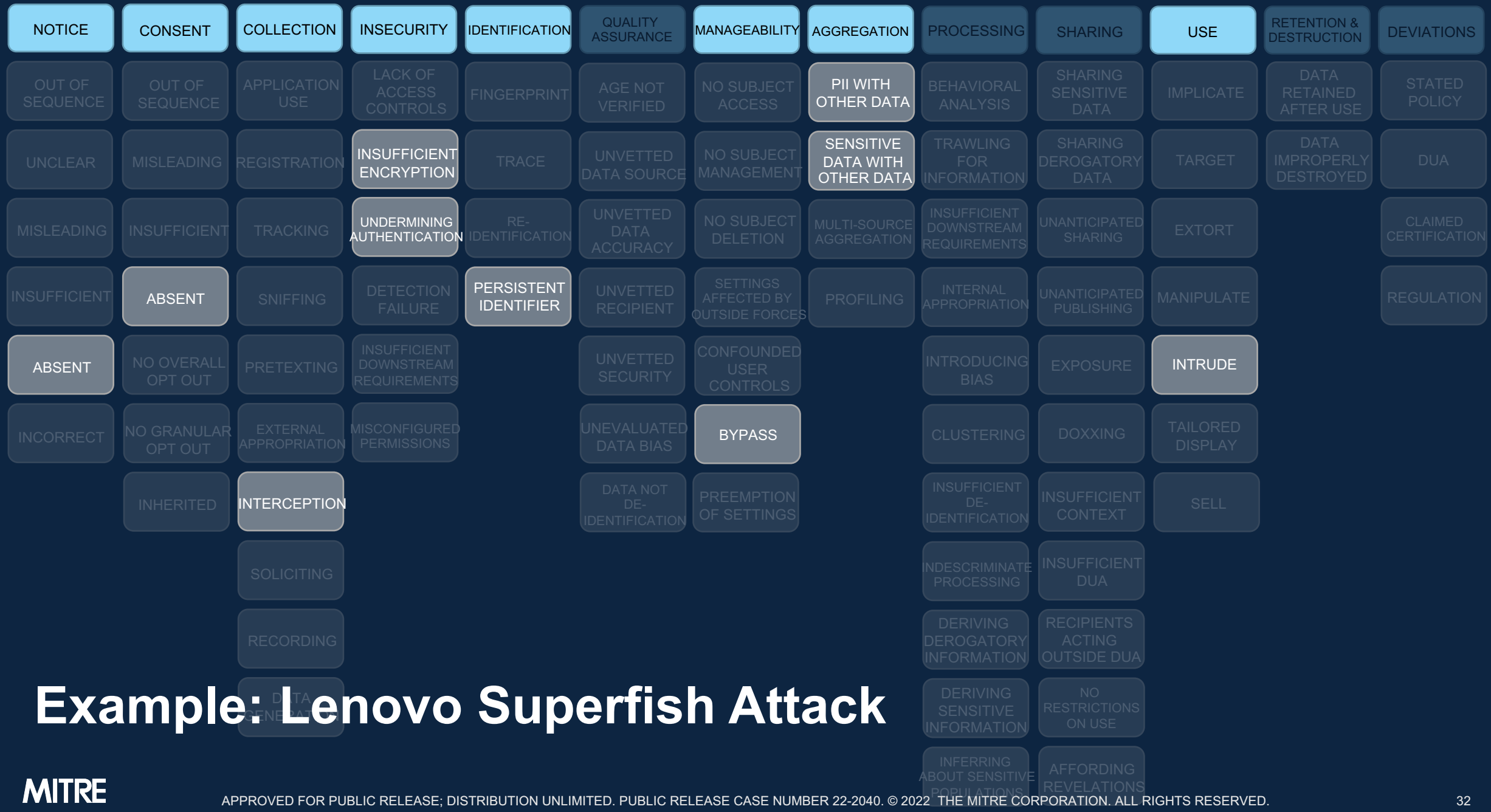


Example: Data De-identification Threat Pattern



Example: Data De-identification Threat Pattern

Example: Lenovo Superfish Attack

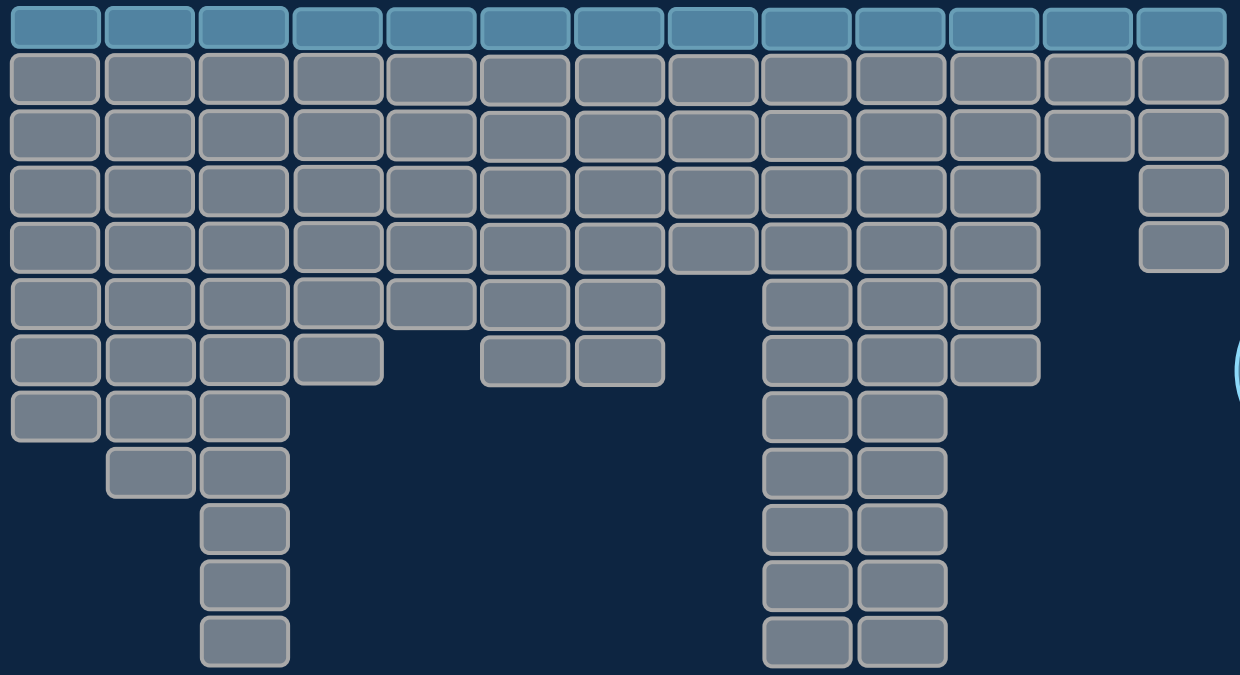


Example: Lenovo Superfish Attack

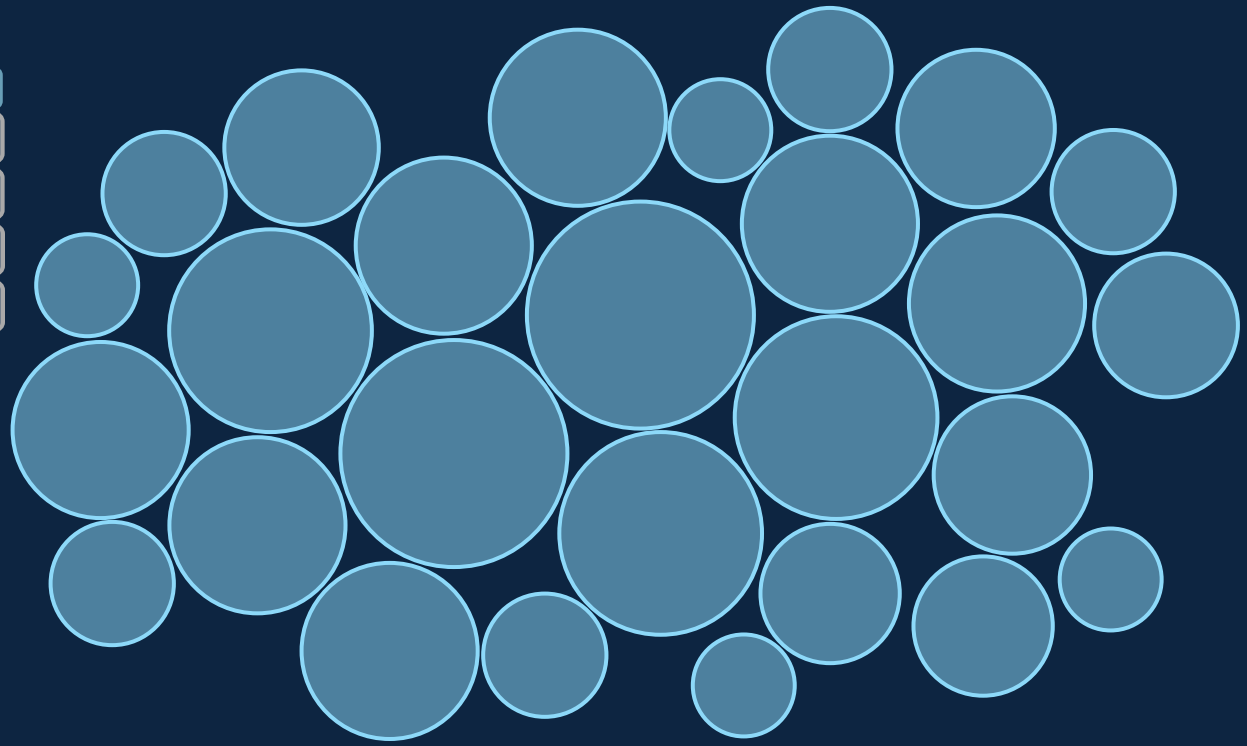
MITRE

CURRENT STATUS – Two prototypes

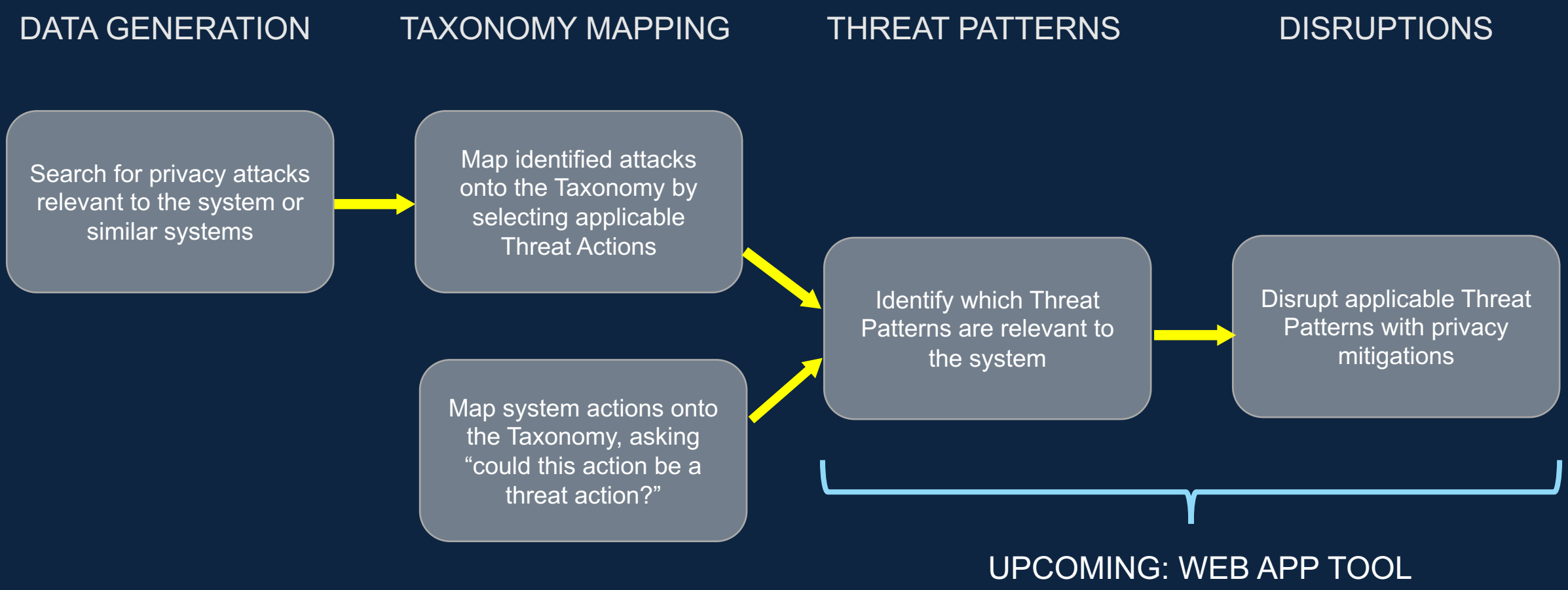
Privacy Threat Taxonomy



Privacy Threat Patterns



THREAT MODELING



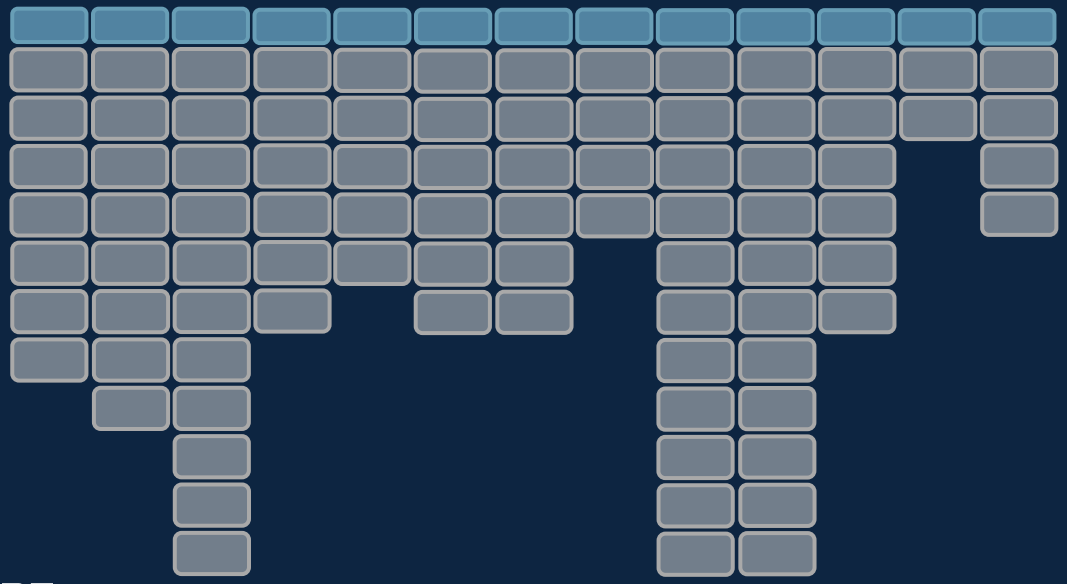
RISK MODELING

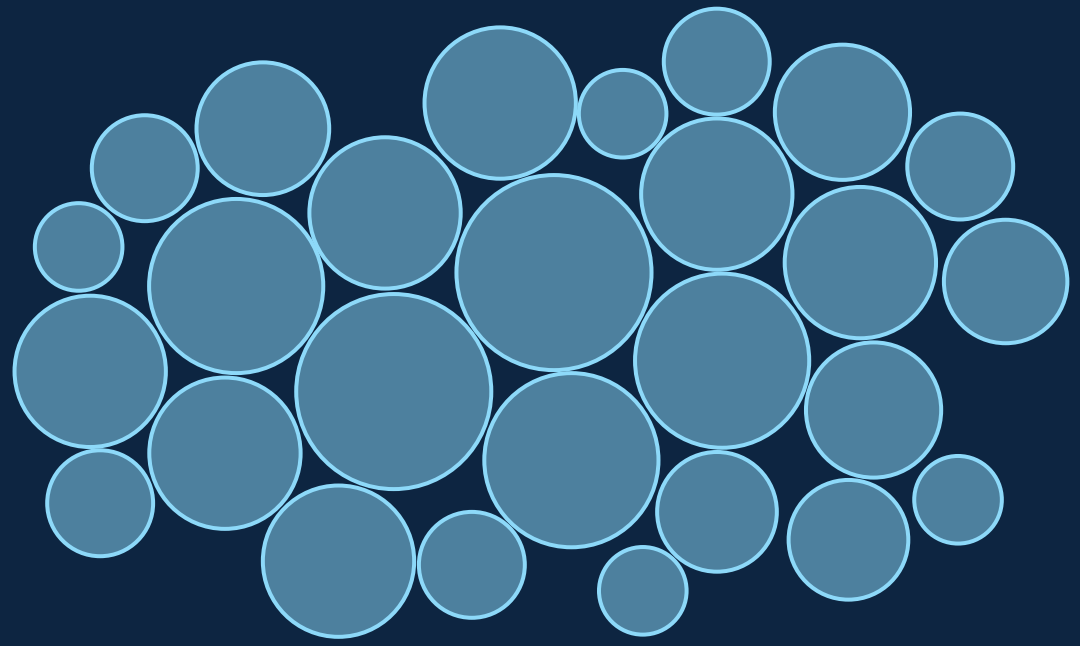
Risk = f(Threats, Vulnerabilities, Consequences)

- By asking what Actions can be Threat Actions, you have a better understanding of how vulnerabilities can be exploited
- Organizations can focus mitigation efforts on known threats or the most high-risk threats to system

NEXT STEPS – Stabilize the prototypes

- Finish first iteration of Taxonomy and Threat Pattern generation
- Generate new dataset of privacy attacks found in news publications
- Map attacks to Privacy Threat Taxonomy and adjust Taxonomy as needed
- Categorize attacks using Privacy Threat Clusters and adjust Patterns as needed





MITRE

Get involved!

We are looking for:

- Datasets or information about privacy attacks (non-breach privacy events)
- Partners to beta test the taxonomy in their privacy program
- Experts to give feedback on the Taxonomy Activities and Threat Actions

Join us at our Privacy Threat Modeling Workshop at the Symposium on Usable Privacy and Security (SOUPS) August 7th in Boston

http://ptmworkshop.gitlab.io

Join our mailing list or get more info on our workshop

ptmworkshop@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Cara Bloom

carabloom.com

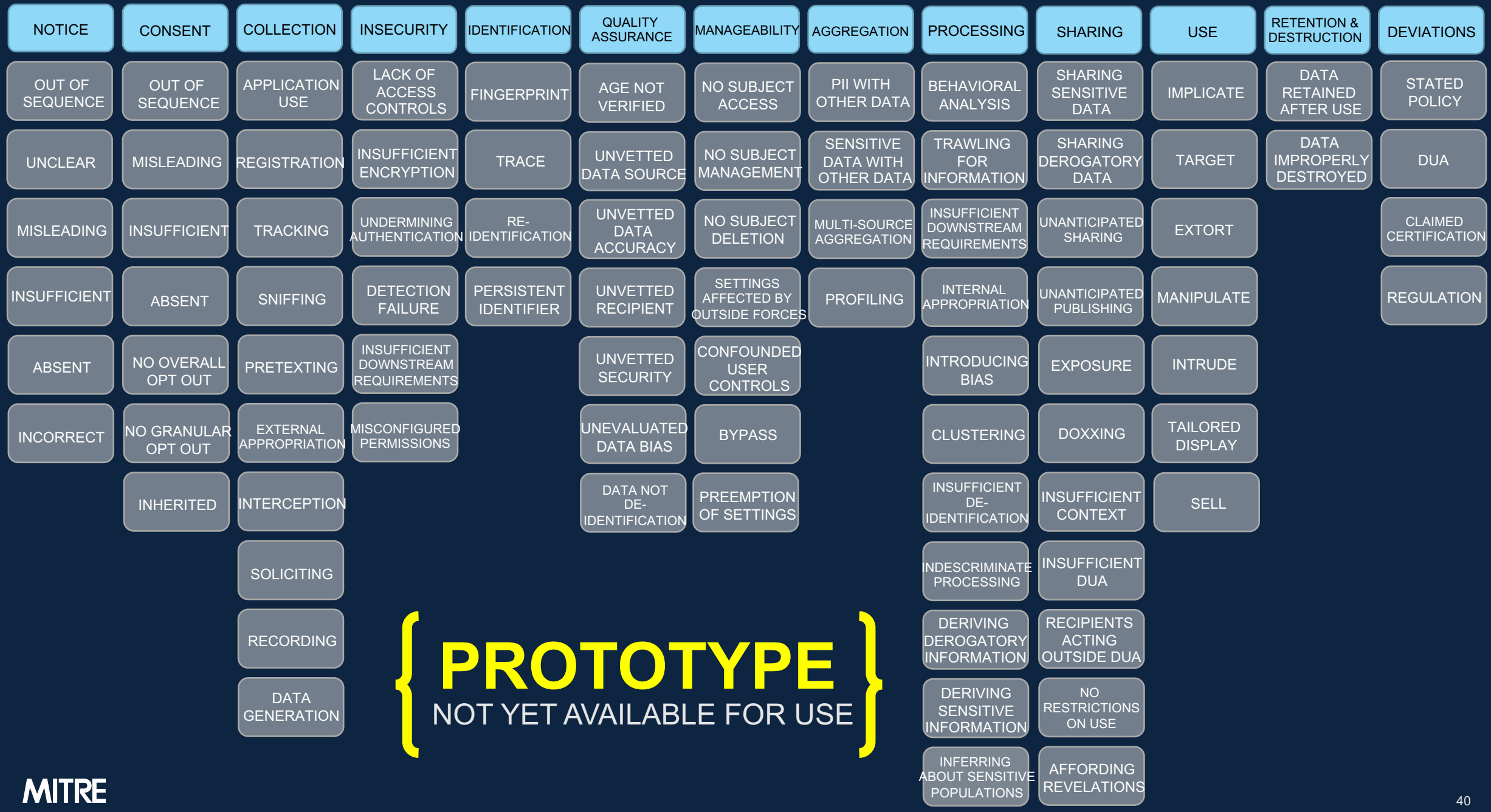
cbloom@mitre.org

@caracbloom

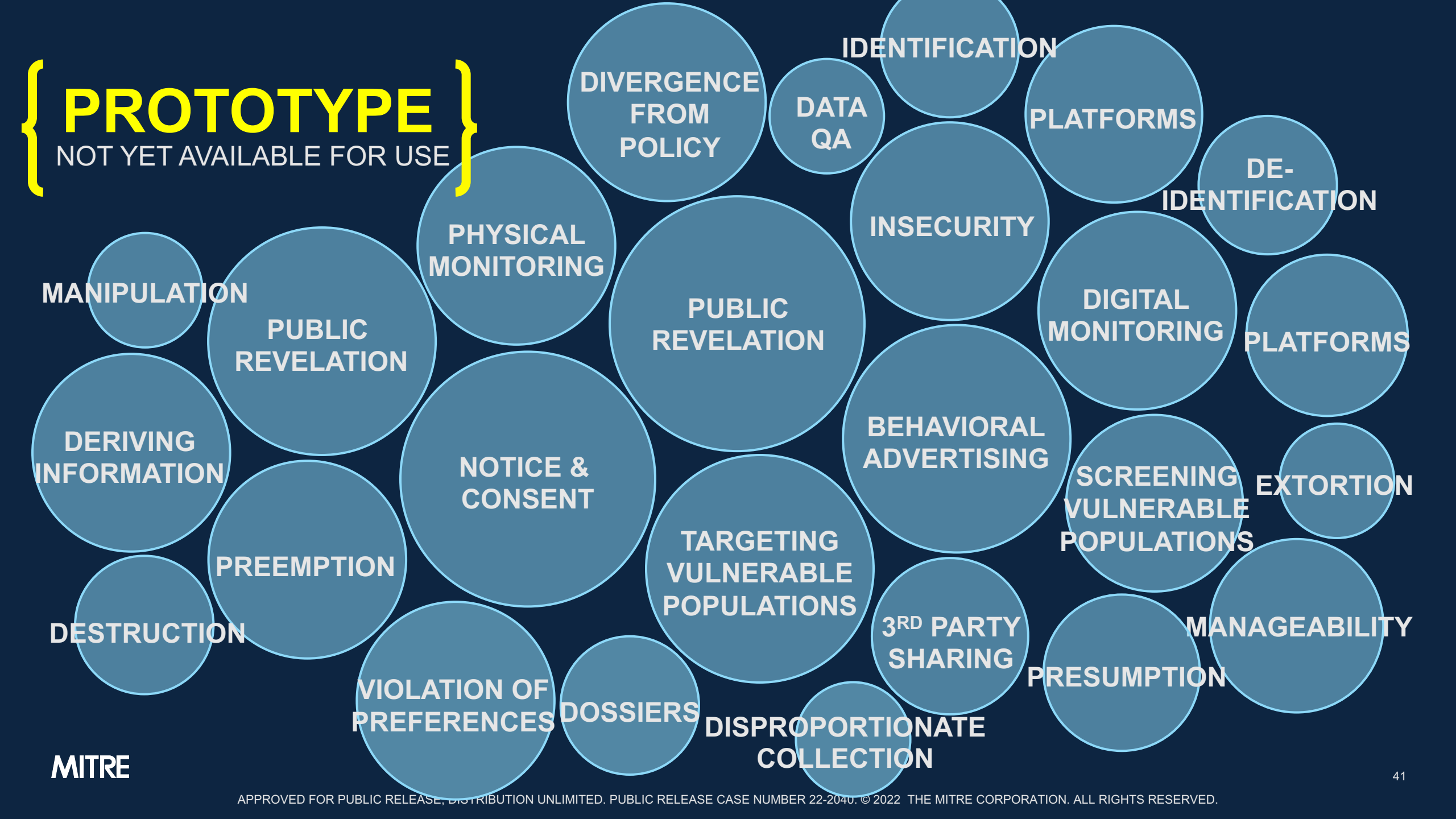
Linkedin.com/in/carabloom

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

BACKUP



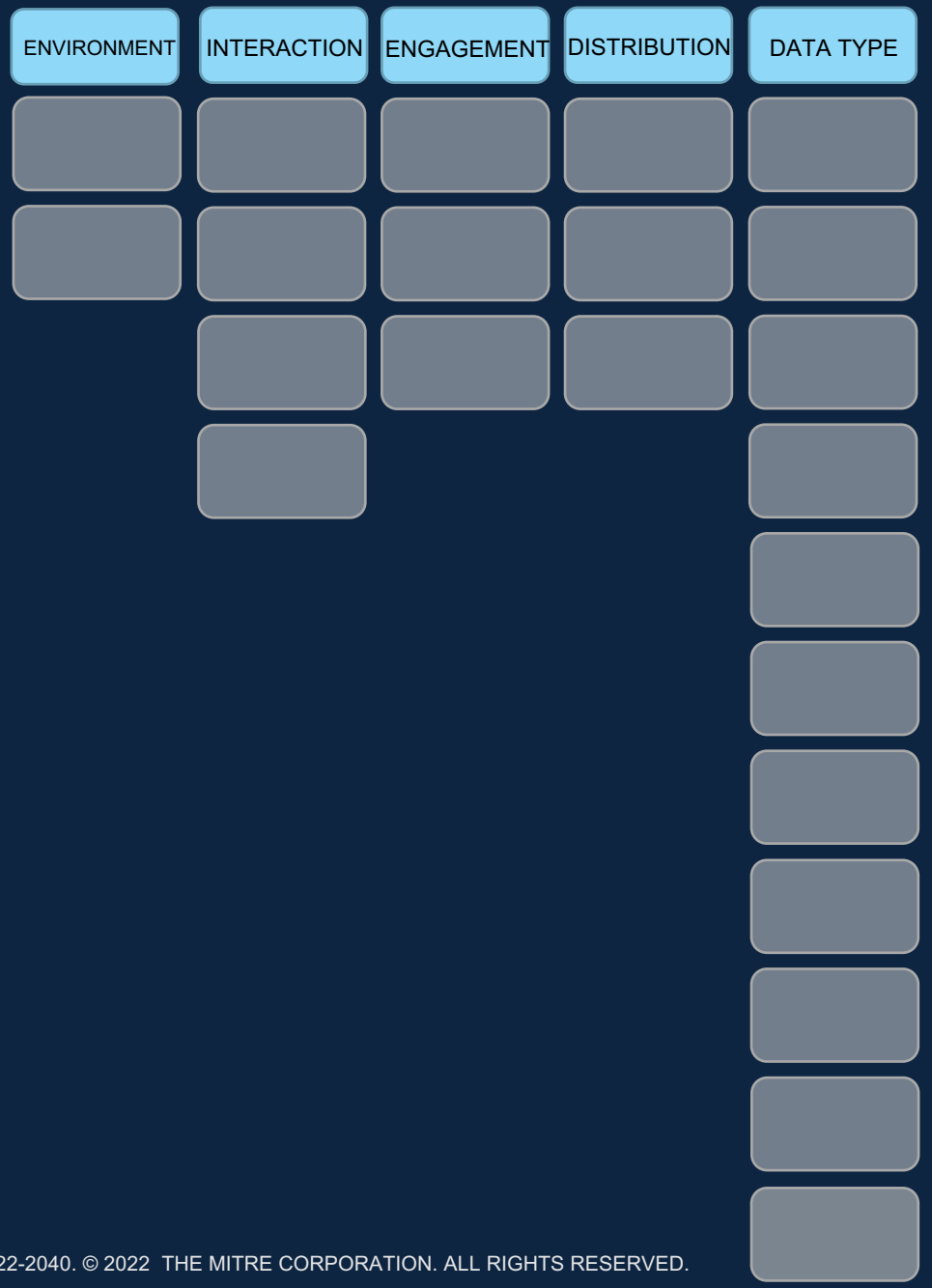
MITRE



MITRE

SOCIO-TECHNICAL CONTEXT

- Information outside the attack killchain that informs the threat level



SOCIO-TECHNICAL CONTEXT

- Information outside the attack killchain that informs the threat level