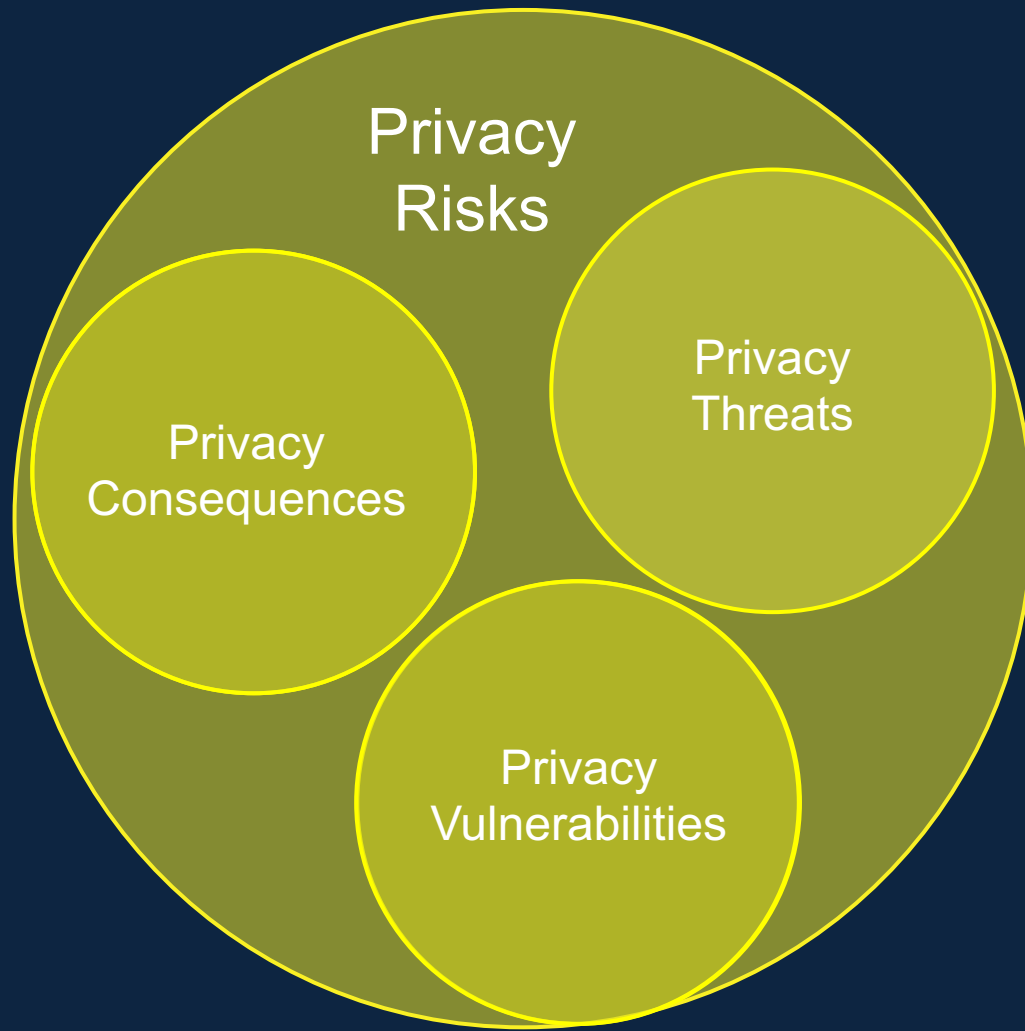


Privacy Threat Modeling

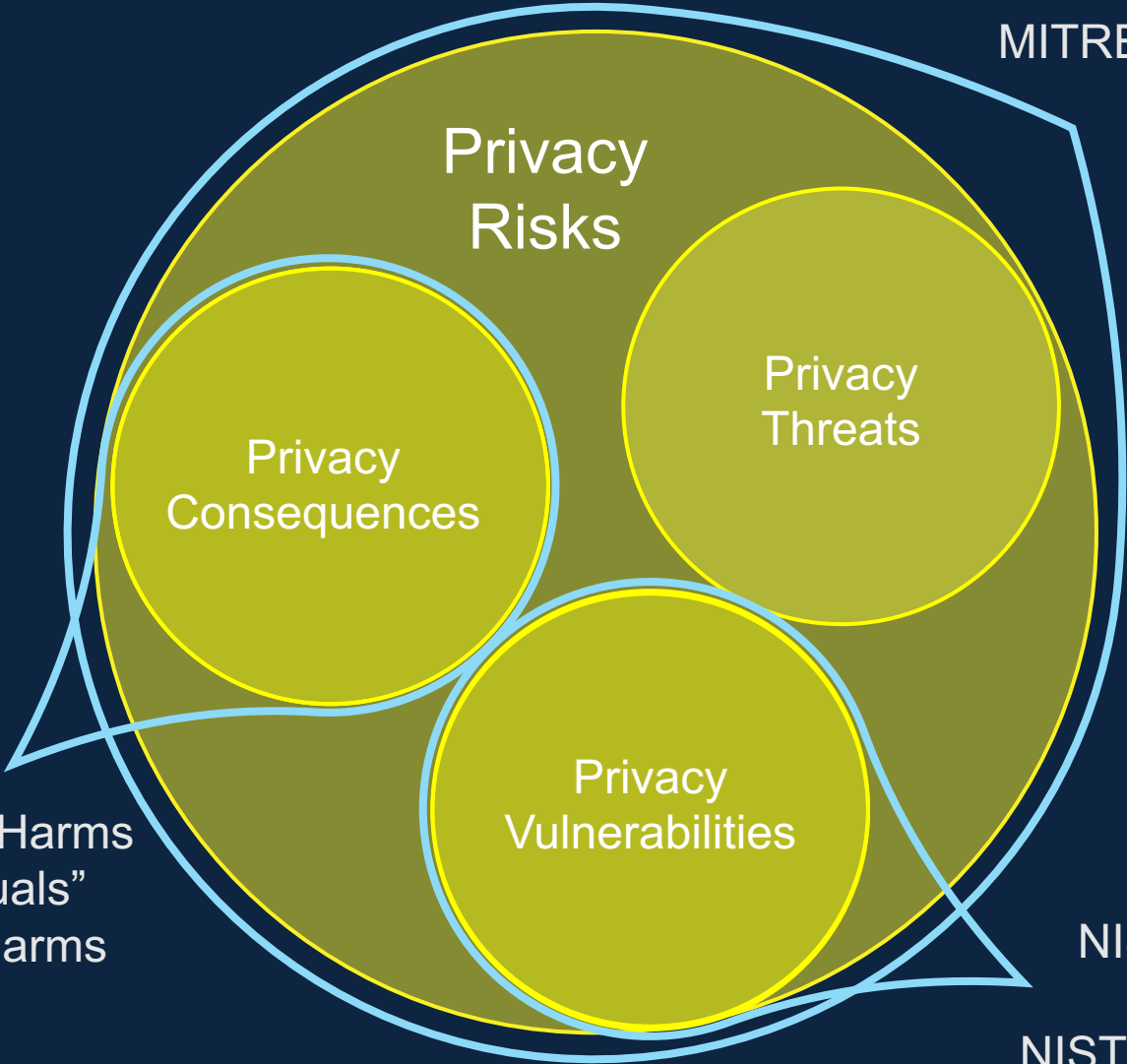
PEPR, June 2022

Cara Bloom

MITRE

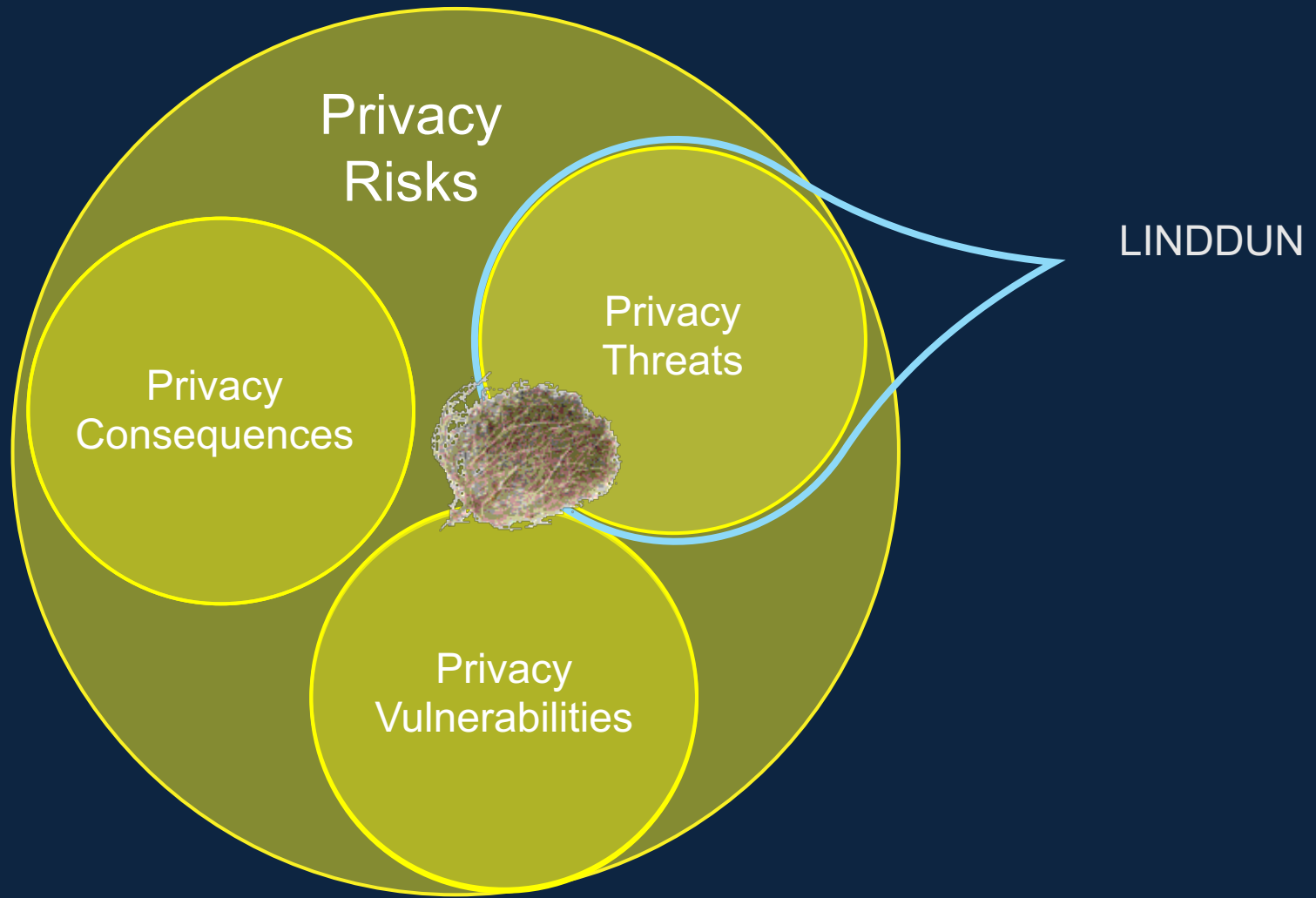


NIST Privacy Risk Assessment Methodology
NIST Privacy Framework
MITRE Privacy Engineering Tools
FAIR-P



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

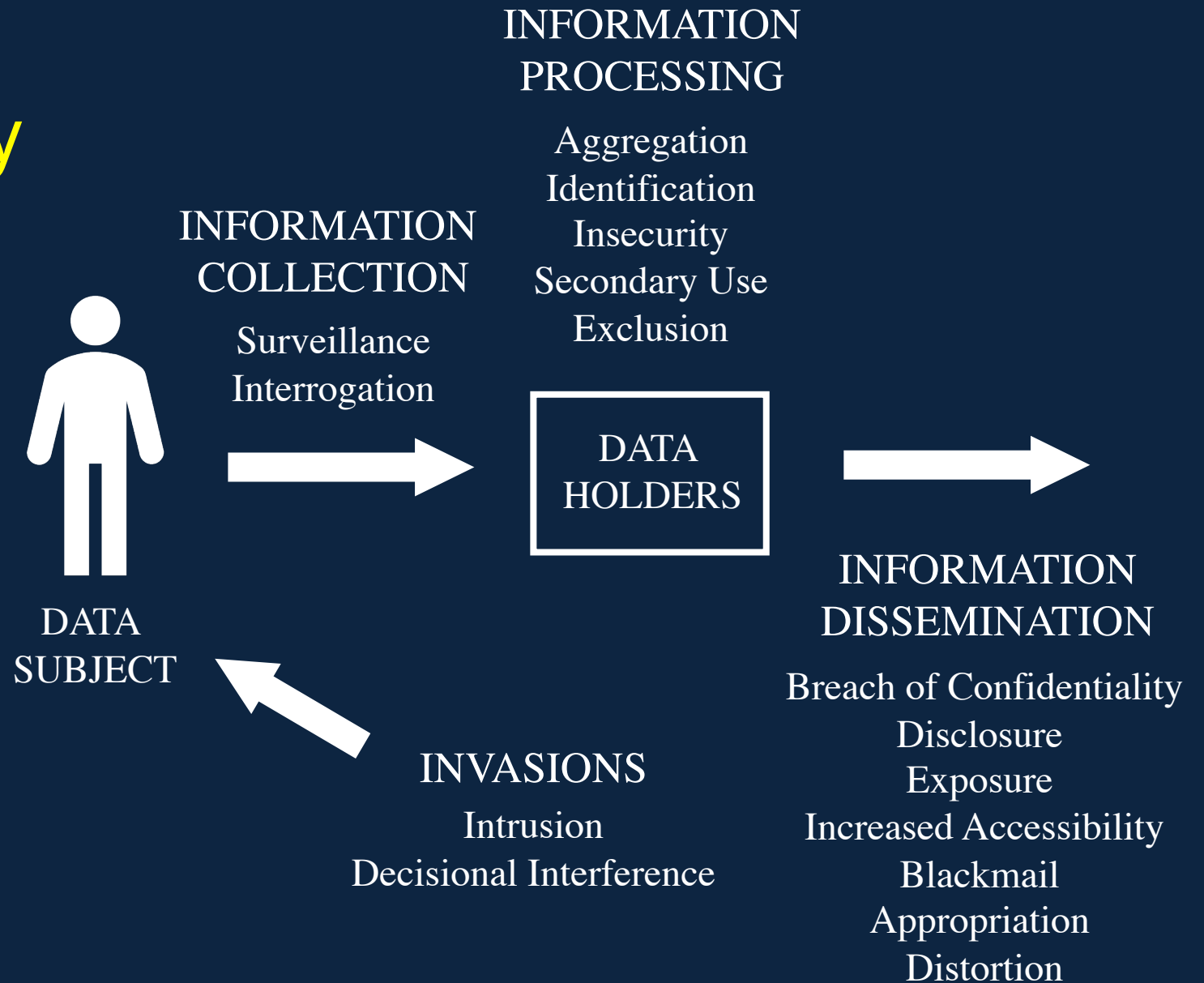


Privacy Attack:

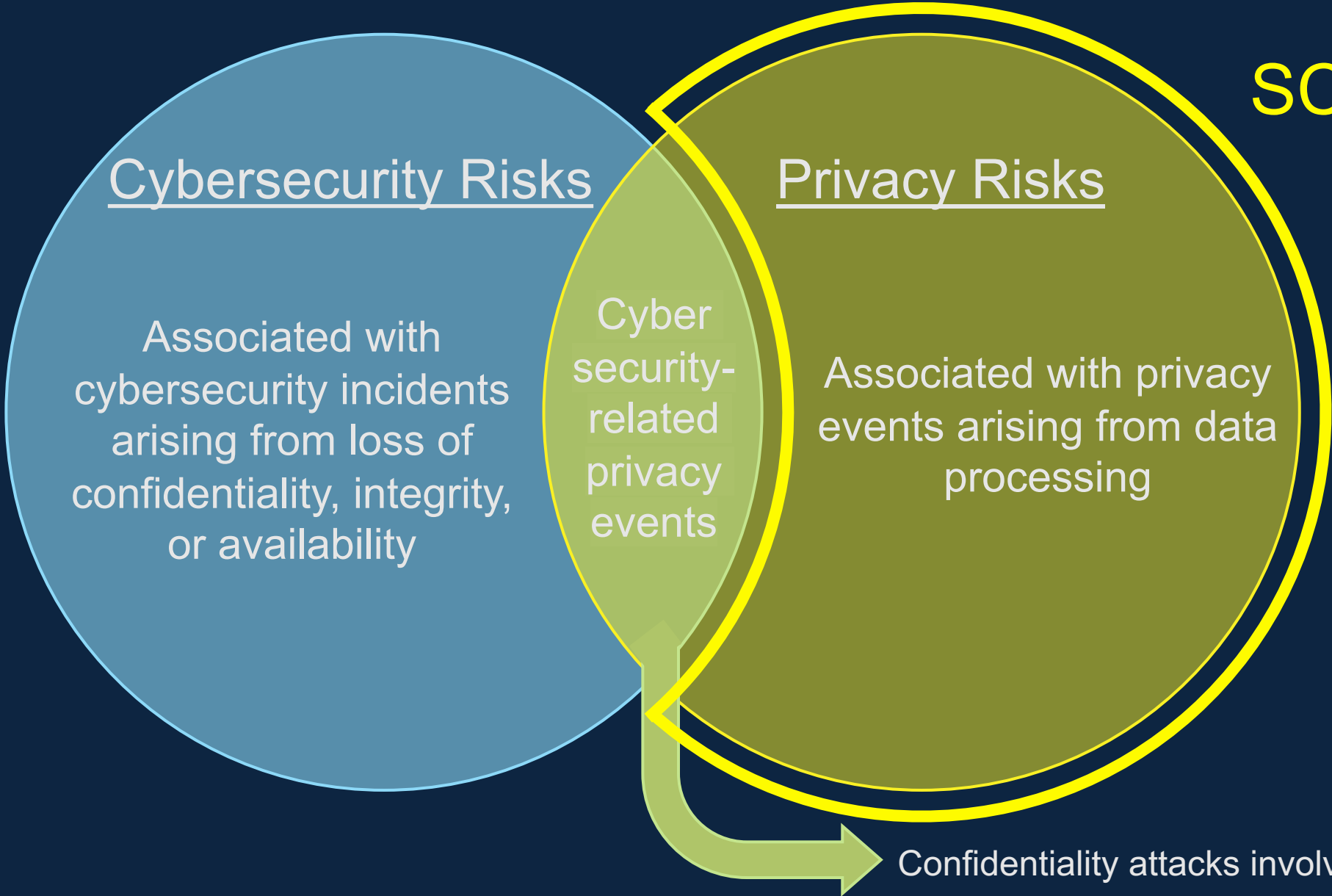
Actions or inactions that cause a perceived privacy harm*, that do not solely involve cybersecurity violations

*As defined by Solove's Taxonomy

Solove's Taxonomy of Privacy (Harms)



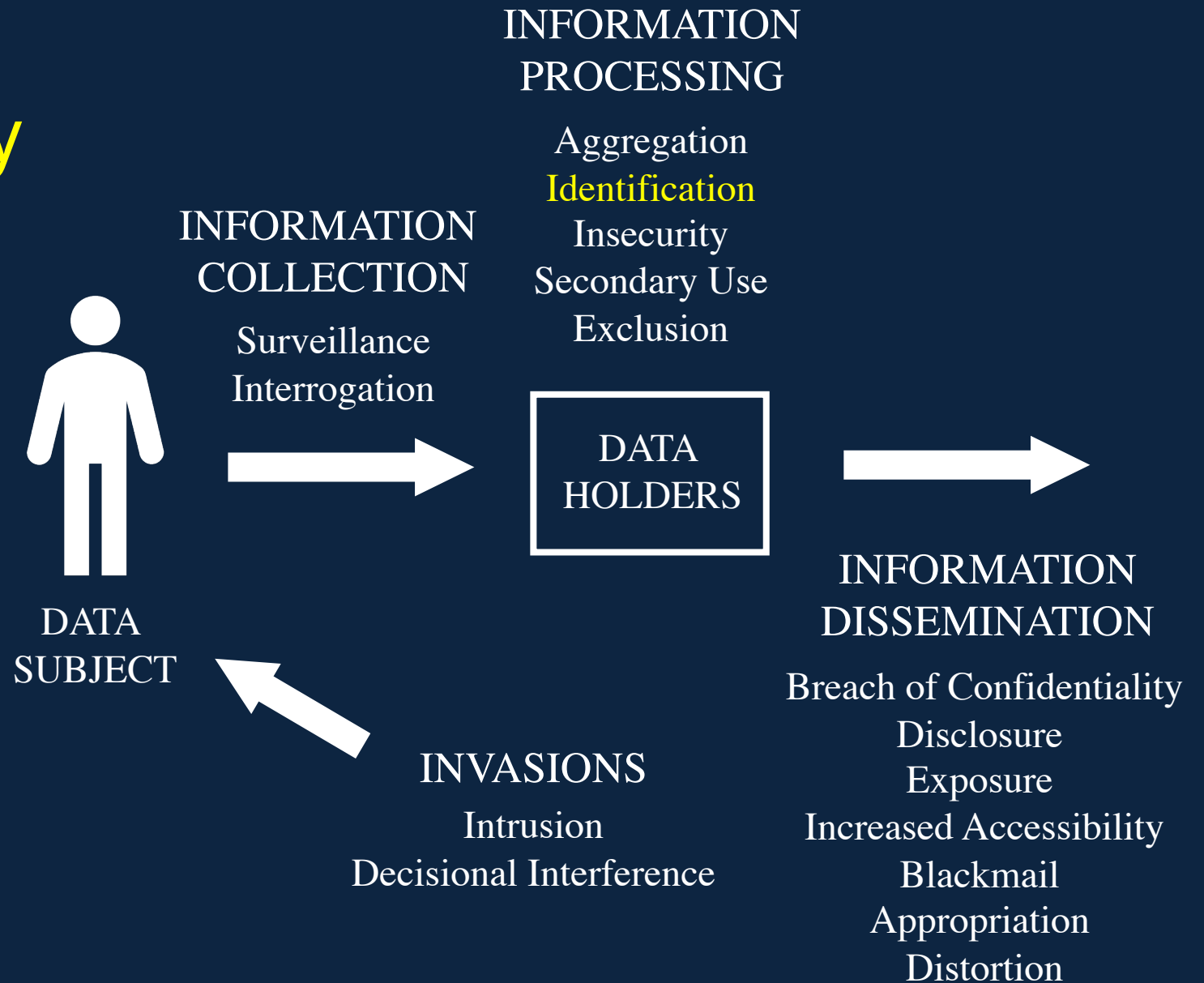
SCOPE





Washington Health Identification

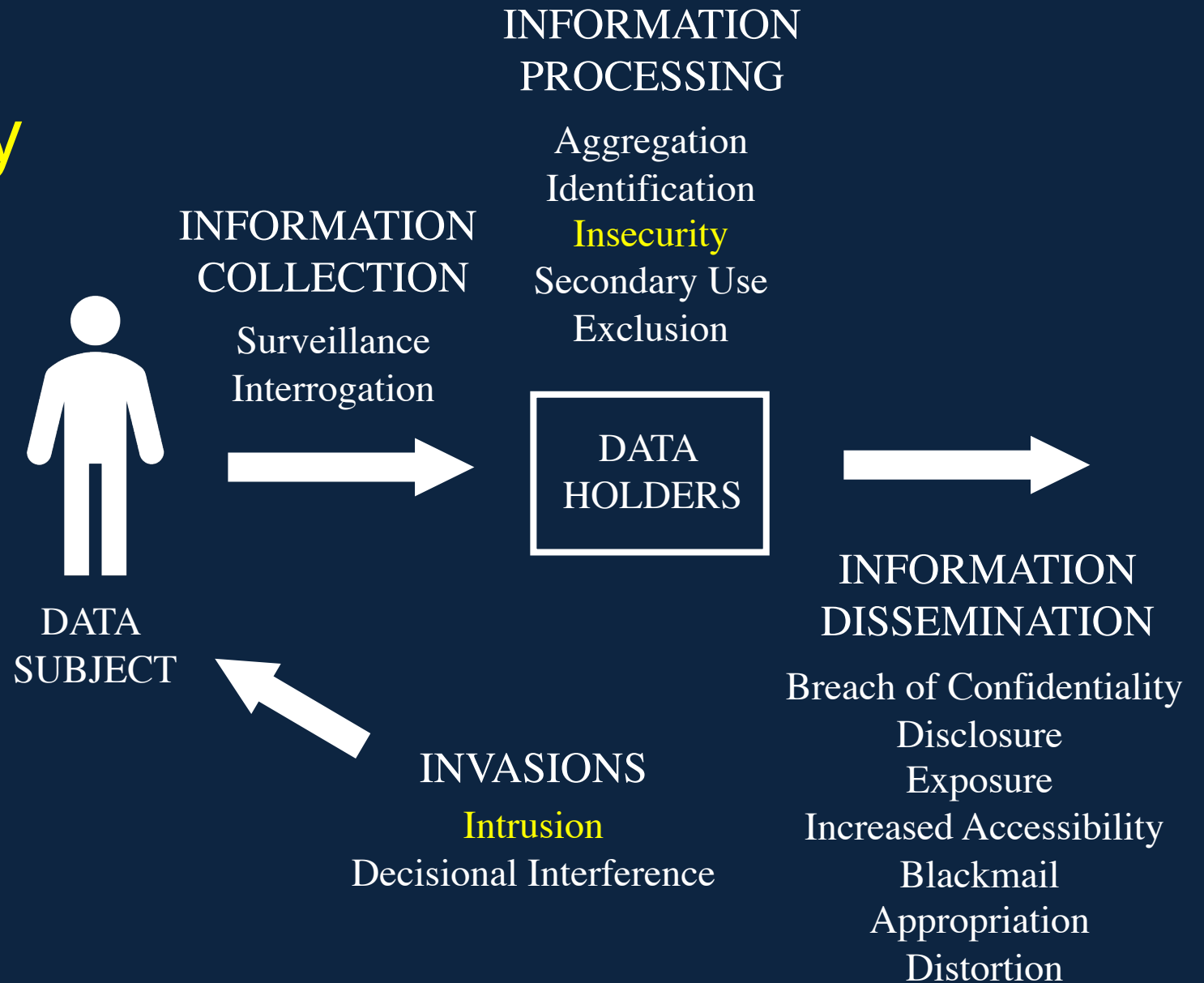
Solove's Taxonomy of Privacy (Harms)



Lenovo Superfish Insecurity & Intrusion



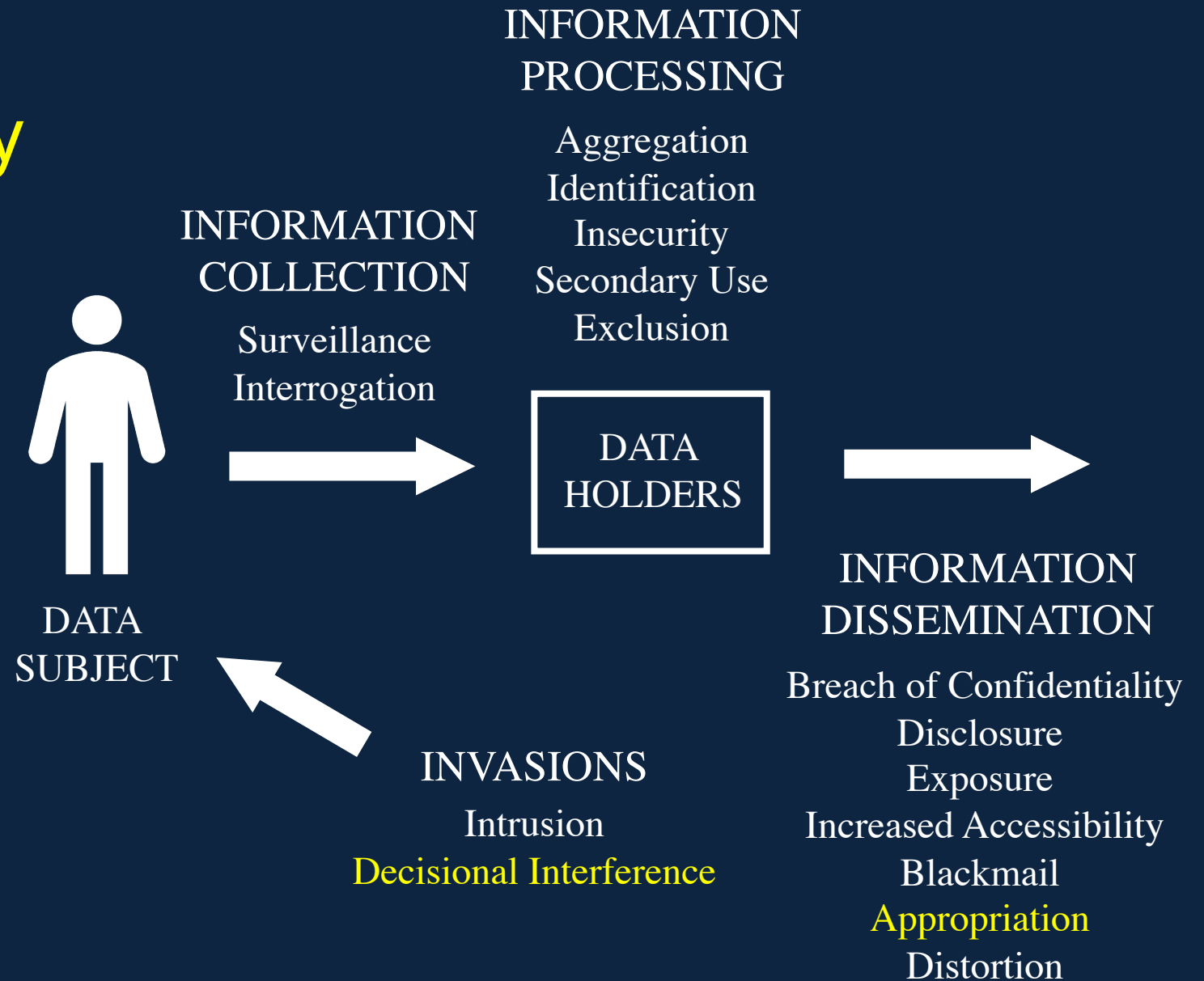
Solove's Taxonomy of Privacy (Harms)



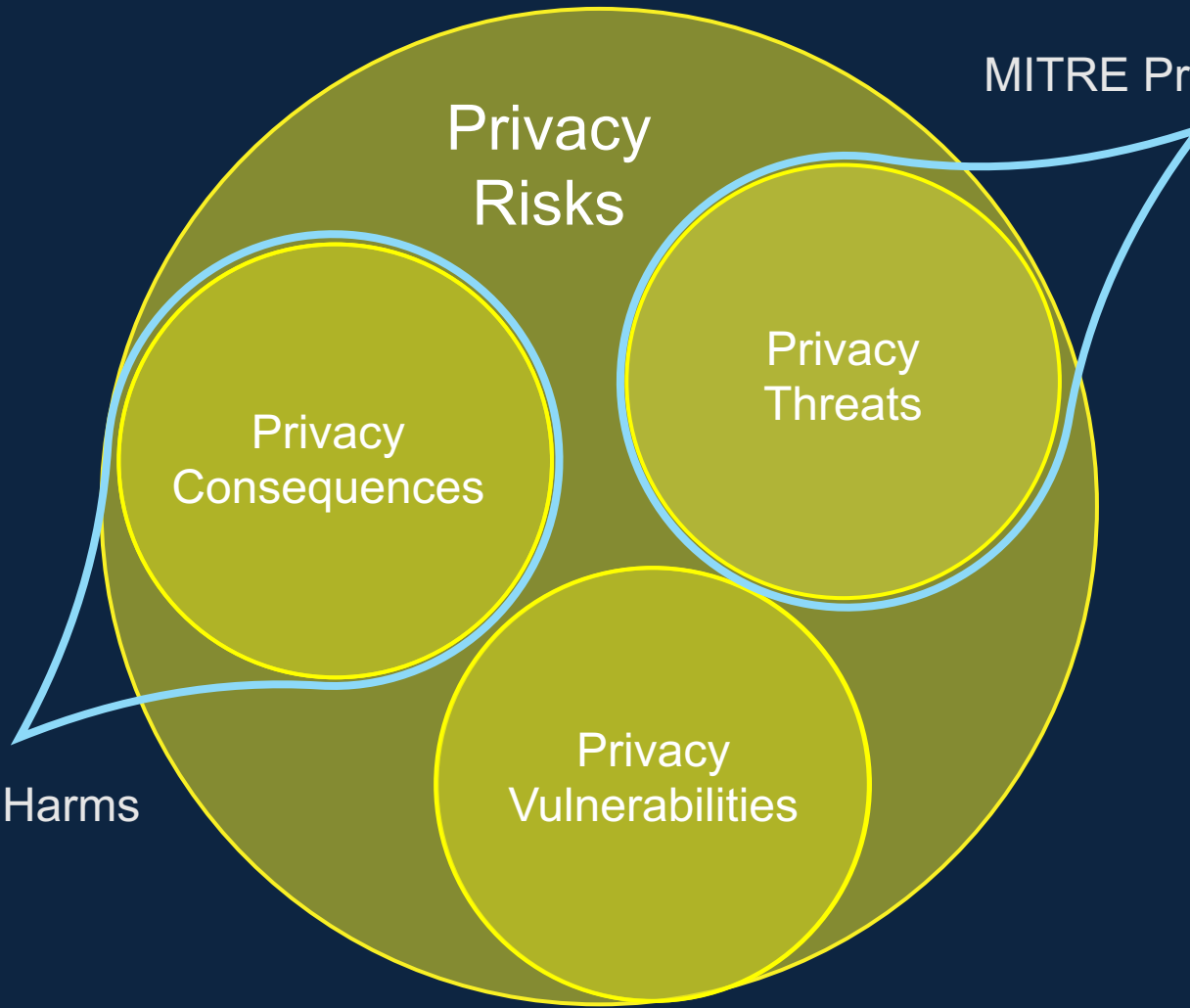


Cambridge Analytica Appropriation & Decisional Interference

Solove's Taxonomy of Privacy (Harms)



MITRE Privacy Threat Taxonomy



Privacy Risks

Privacy Threats

Privacy Consequences

Privacy Vulnerabilities

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

Cambridge Analytica

2013-2018

Several million Facebook users

Washington Health

2013

Unknown

Venmo

2011-2018

Unknown

Equifax Information Services

2008-2010

Several million users

Retina-X Studios

2007-2020

>15,300 users

Iconix COPPA

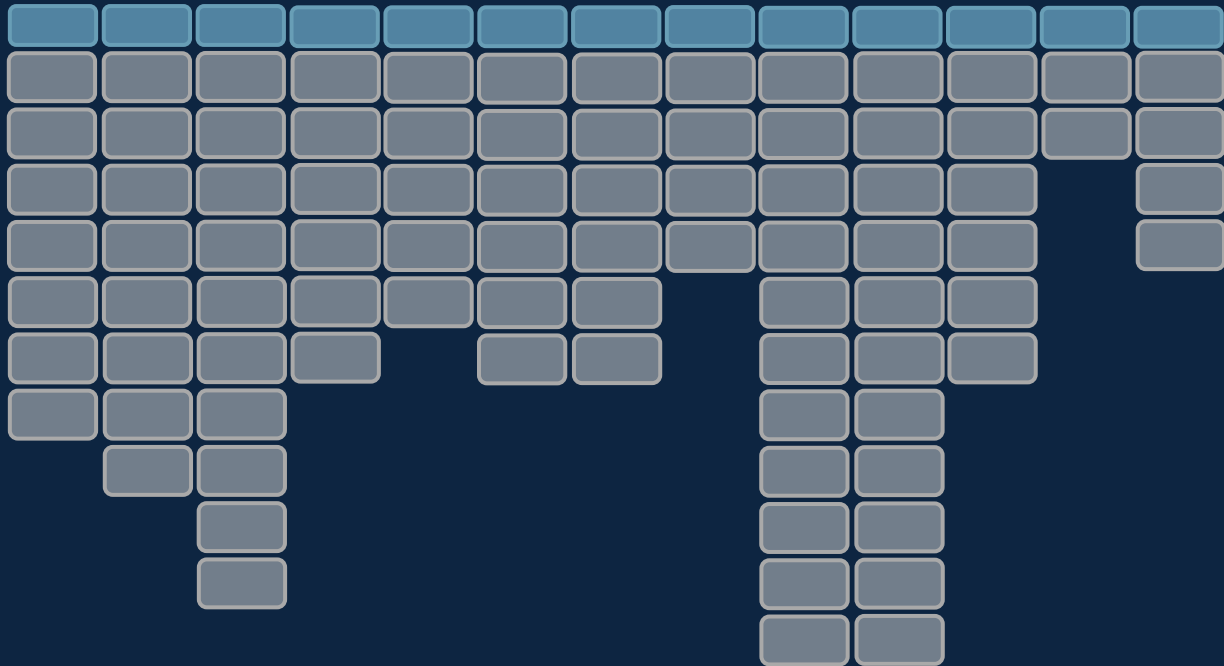
2006-2009

~1000 children

Personal stories & photos

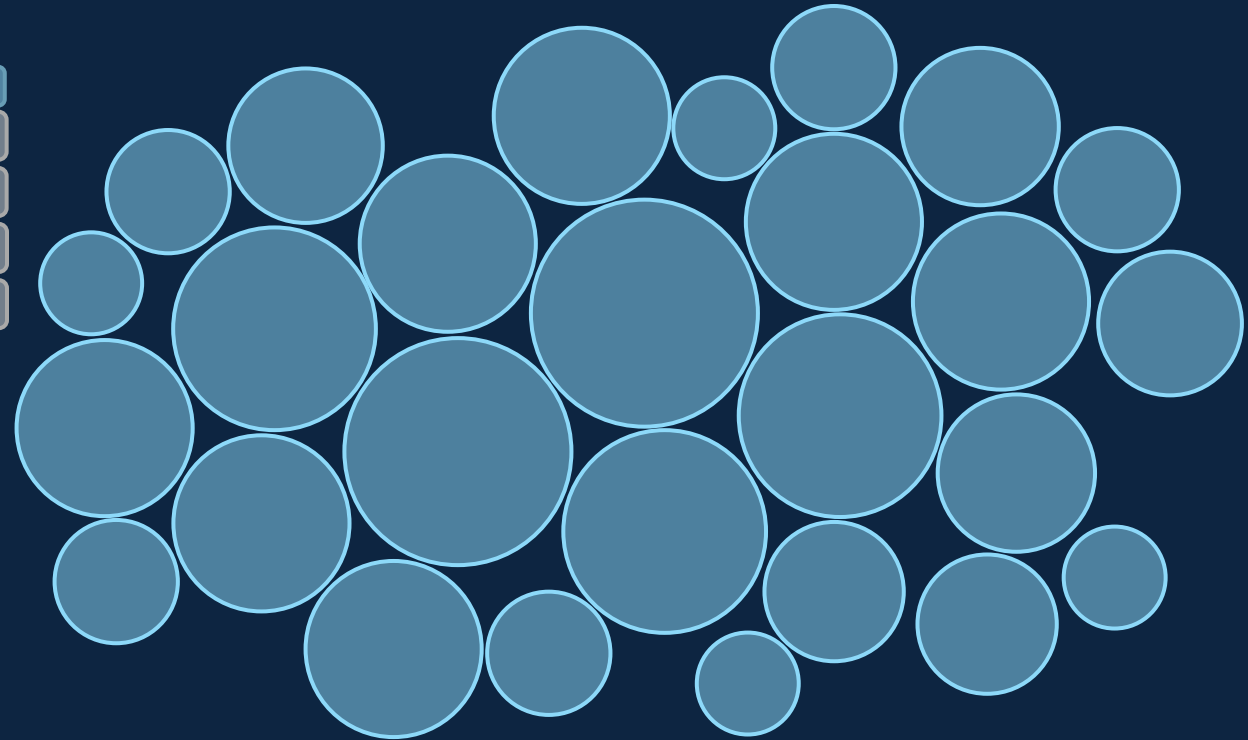
PROTOTYPES

Privacy Threat Taxonomy



Hierarchical ontology of attack components

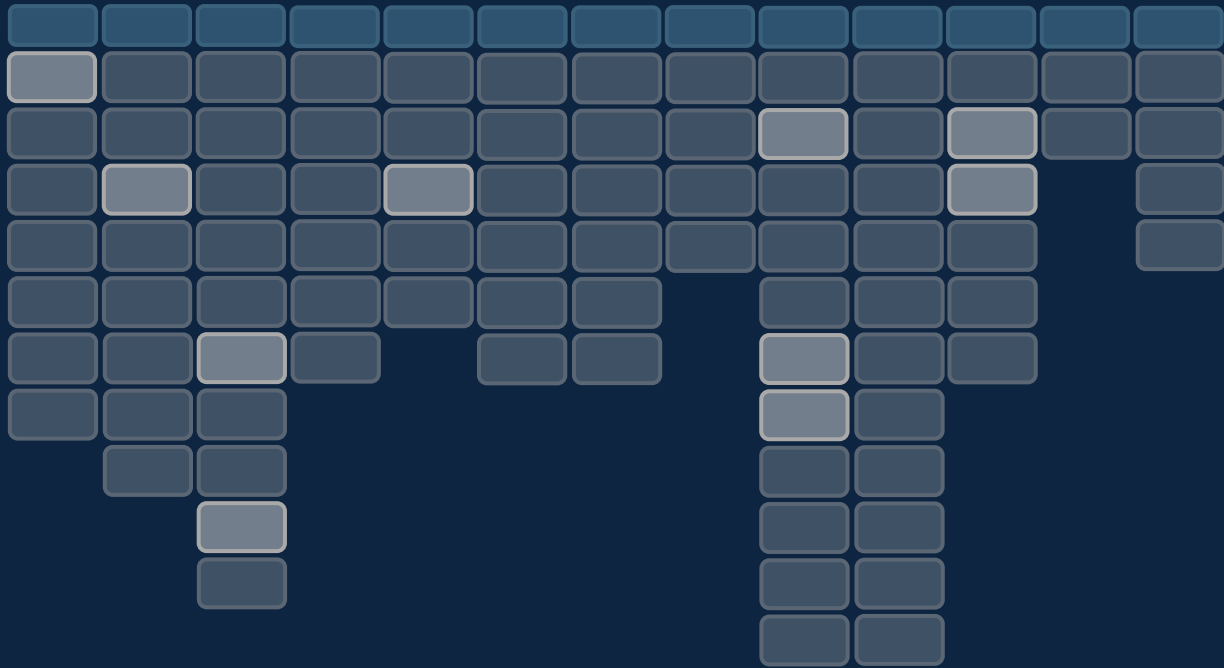
Privacy Threat Clusters



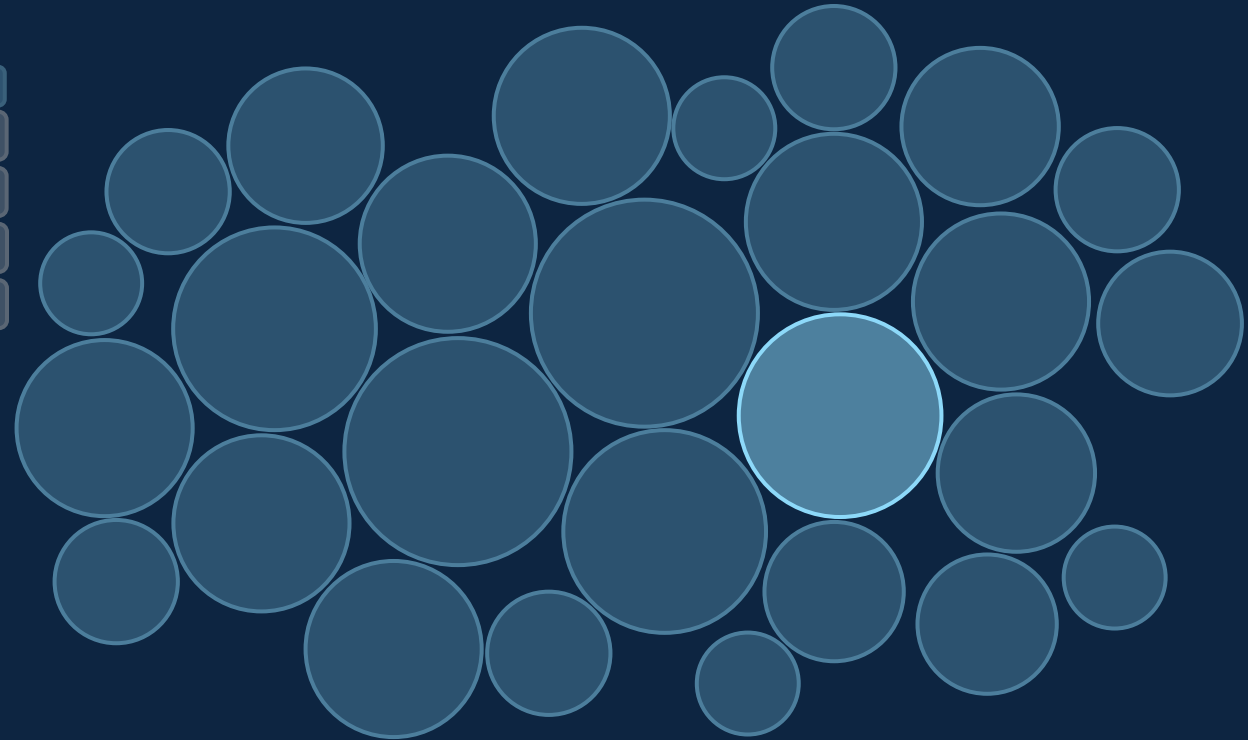
Typology of attacks

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**

COLLECTION

ACTIVITY



EXPOSURE

THREAT
ACTION



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

NOTICE	CONSENT	COLLECTION	INSECURITY	IDENTIFICATION	QUALITY ASSURANCE	MANAGEABILITY	AGGREGATION	PROCESSING	SHARING	USE	RETENTION & DESTRUCTION	DEVIATIONS
		APPLICATION USE										
		REGISTRATION										
		TRACKING										
		SNIFFING										
		PRETEXTING										
		EXTERNAL APPROPRIATION										
		INTERCEPTION										
		SOLICITING										
		RECORDING										
		DATA GENERATION										

CLUSTERING

MANAGEABILITY

DIVERGENCE FROM POLICY

IDENTIFICATION

DATA QA

PLATFORMS

DE-IDENTIFICATION

PHYSICAL MONITORING

INSECURITY

MANIPULATION

PUBLIC REVELATION

PUBLIC REVELATION

DIGITAL MONITORING

PLATFORMS

DERIVING INFORMATION

CLUSTERING

JUSTICE
CONSENT

SCREENING VULNERABLE POPULATIONS

PREEMPTION

TARGETING VULNERABLE POPULATIONS

DESTRUCTION

3RD PARTY SHARING

EXTORTION

VIOLATION OF PREFERENCES

DOSSIERS

DISPROPORTIONATE COLLECTION

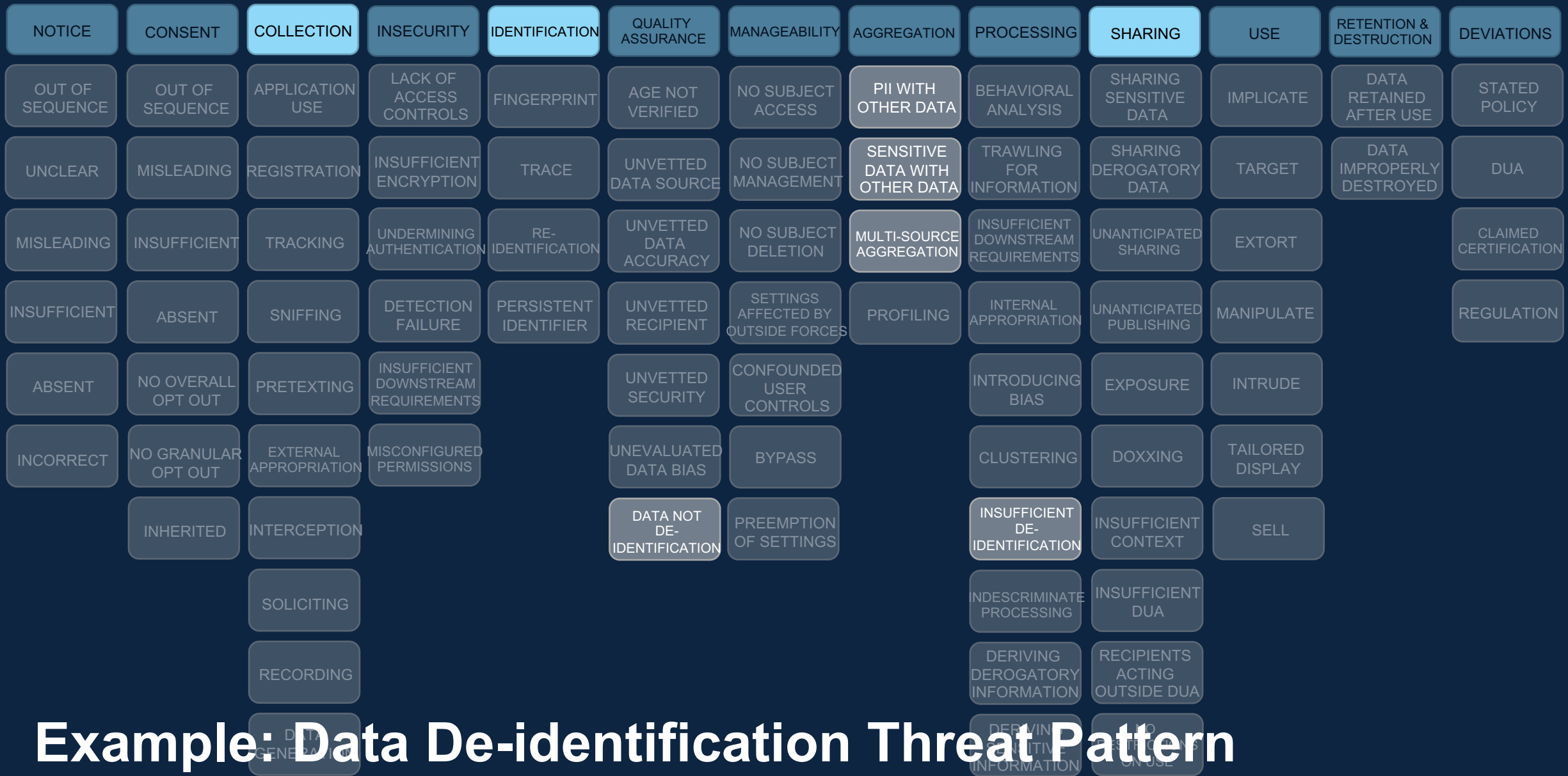
PRESUMPTION

CLUSTERING & THREAT PATTERNS

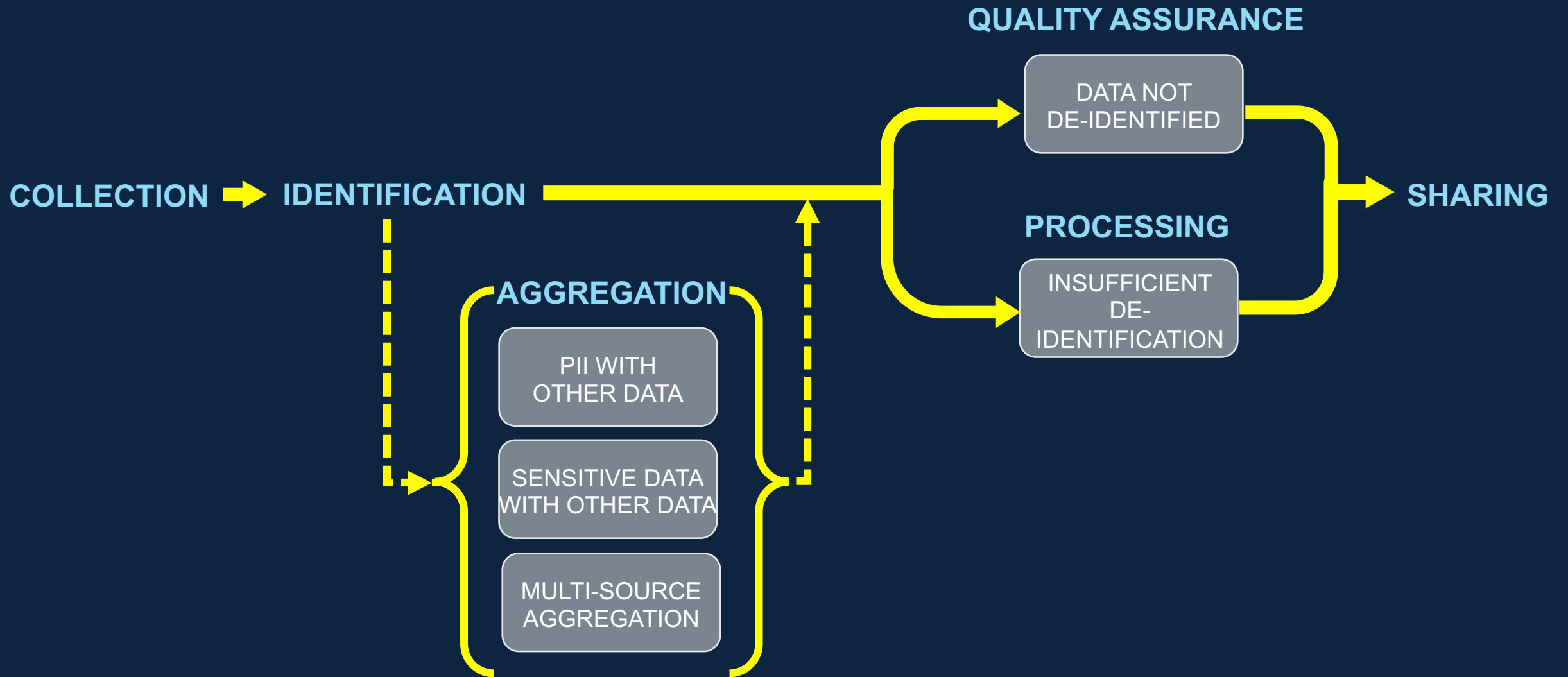
- Break attacks into individual **threat actions**
- Cluster attacks with similar threat actions into **Threat Clusters**
- Map all attacks in dataset to existing groupings, refining and renaming Threat Clusters as needed
- Map each Threat Cluster to the Taxonomy
- Using the threat actions from the taxonomy, 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



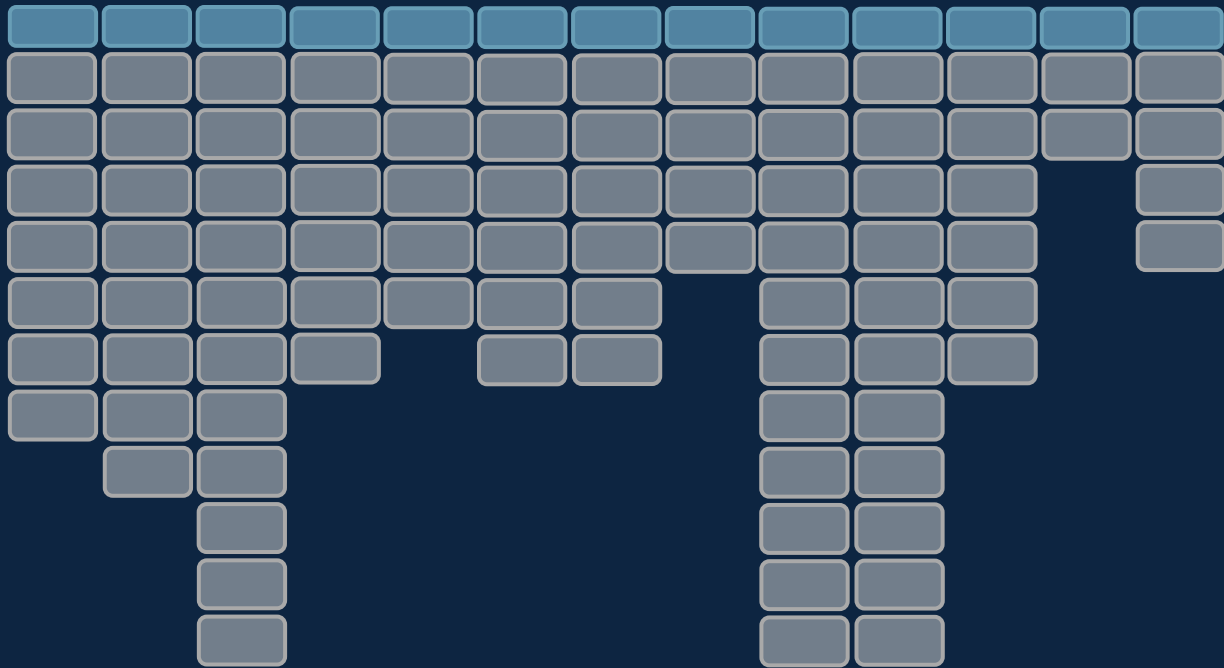
Example: Lenovo Superfish Attack

NOTICE	CONSENT	COLLECTION	INSECURITY	IDENTIFICATION	QUALITY ASSURANCE	MANAGEABILITY	AGGREGATION	PROCESSING	SHARING	USE	RETENTION & DESTRUCTION	DEVIATIONS
OUT OF SEQUENCE	OUT OF SEQUENCE	APPLICATION USE	LACK OF ACCESS CONTROLS	FINGERPRINT	AGE NOT VERIFIED	NO SUBJECT ACCESS	PII WITH OTHER DATA	BEHAVIORAL ANALYSIS	SHARING SENSITIVE DATA	IMPLICATE	DATA RETAINED AFTER USE	STATED POLICY
UNCLEAR	MISLEADING	REGISTRATION	INSUFFICIENT ENCRYPTION	TRACE	UNVETTED DATA SOURCE	NO SUBJECT MANAGEMENT	SENSITIVE DATA WITH OTHER DATA	TRAWLING FOR INFORMATION	SHARING DEROGATORY DATA	TARGET	DATA IMPROPERLY DESTROYED	DUA
MISLEADING	INSUFFICIENT	TRACKING	UNDERMINING AUTHENTICATION	RE-IDENTIFICATION	UNVETTED DATA ACCURACY	NO SUBJECT DELETION	MULTI-SOURCE AGGREGATION	INSUFFICIENT DOWNSTREAM REQUIREMENTS	UNANTICIPATED SHARING	EXTORT		CLAIMED CERTIFICATION
INSUFFICIENT	ABSENT	SNIFFING	DETECTION FAILURE	PERSISTENT IDENTIFIER	UNVETTED RECIPIENT	SETTINGS AFFECTED BY OUTSIDE FORCES	PROFILING	INTERNAL APPROPRIATION	UNANTICIPATED PUBLISHING	MANIPULATE		REGULATION
ABSENT	NO OVERALL OPT OUT	PRETEXTING	INSUFFICIENT DOWNSTREAM REQUIREMENTS		UNVETTED SECURITY	CONFOUNDED USER CONTROLS		INTRODUCING BIAS	EXPOSURE	INTRUDE		
INCORRECT	NO GRANULAR OPT OUT	EXTERNAL APPROPRIATION	MISCONFIGURED PERMISSIONS		UNEVALUATED DATA BIAS	BYPASS		CLUSTERING	DOXXING	TAILORED DISPLAY		
	INHERITED	INTERCEPTION			DATA NOT DE-IDENTIFICATION	PREEMPTION OF SETTINGS		INSUFFICIENT DE-IDENTIFICATION	INSUFFICIENT CONTEXT	SELL		
		SOLICITING						INDESCRIMINATE PROCESSING	INSUFFICIENT DUA			
		RECORDING						DERIVING DEROGATORY INFORMATION	RECIPIENTS ACTING OUTSIDE DUA			
		DATA GENERATED						DERIVING SENSITIVE INFORMATION	NO RESTRICTIONS ON USE			
								INFERRING ABOUT SENSITIVE POPULATIONS	AFFORDING REVELATIONS			

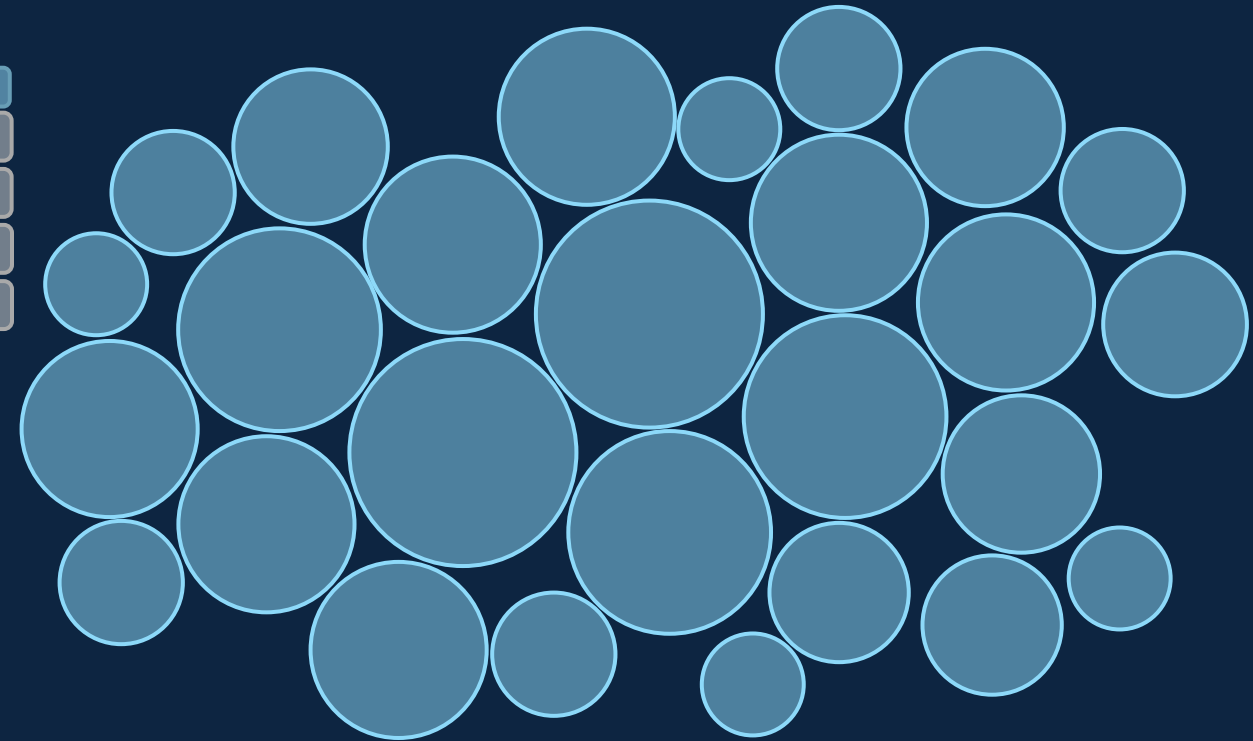
Example: Lenovo Superfish Attack

CURRENT STATUS – Two prototypes

Privacy Threat Taxonomy



Privacy Threat Patterns



THREAT MODELING

DATA GENERATION

Search for privacy attacks relevant to the system or similar systems

TAXONOMY MAPPING

Map identified attacks onto the Taxonomy by selecting applicable Threat Actions

Map system actions onto the Taxonomy, asking "could this action be a threat action?"

THREAT PATTERNS

Identify which Threat Patterns are relevant to the system

DISRUPTIONS

Disrupt applicable Threat Patterns with privacy mitigations

UPCOMING: WEB APP TOOL

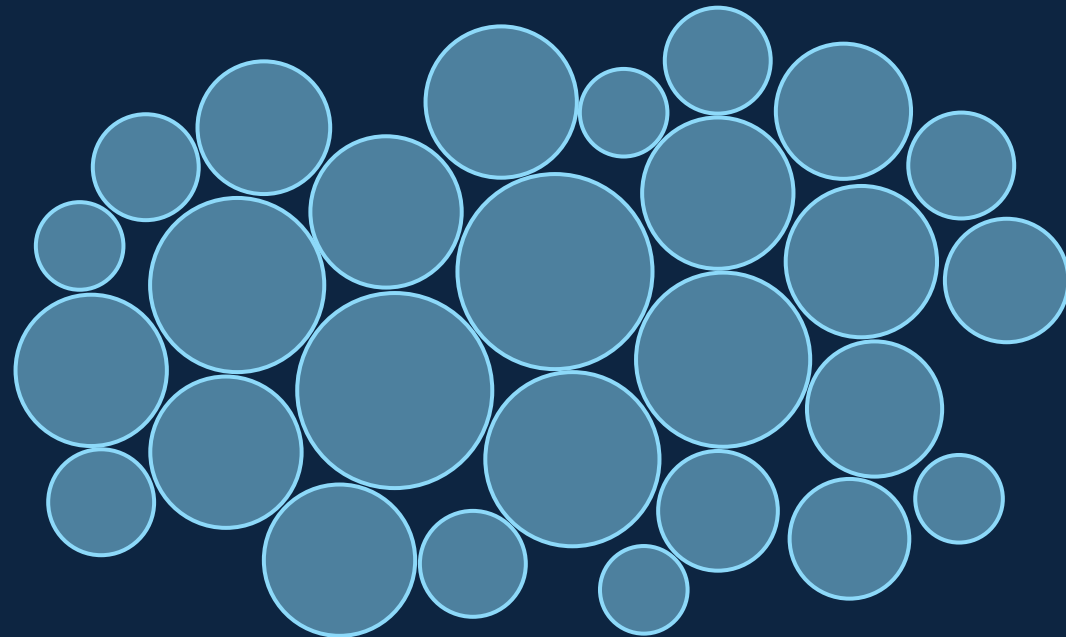
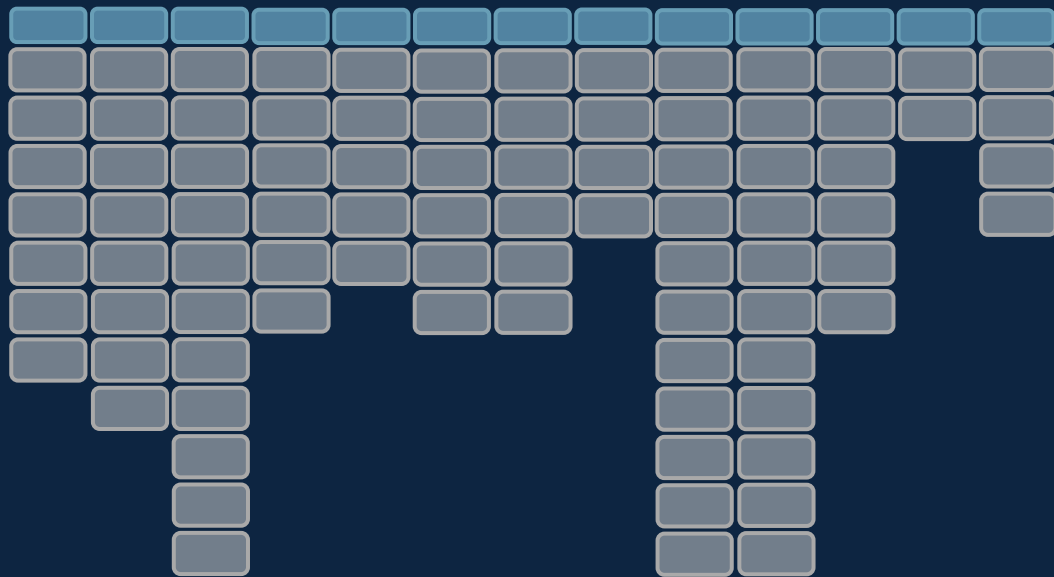
RISK MODELING

$$\text{Risk} = f(\text{Threats}, \text{Vulnerabilities}, \text{Consequences})$$

- 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



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](https://twitter.com/@caracbloom)



[Linkedin.com/in/carabloom](https://www.linkedin.com/in/carabloom)

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD®

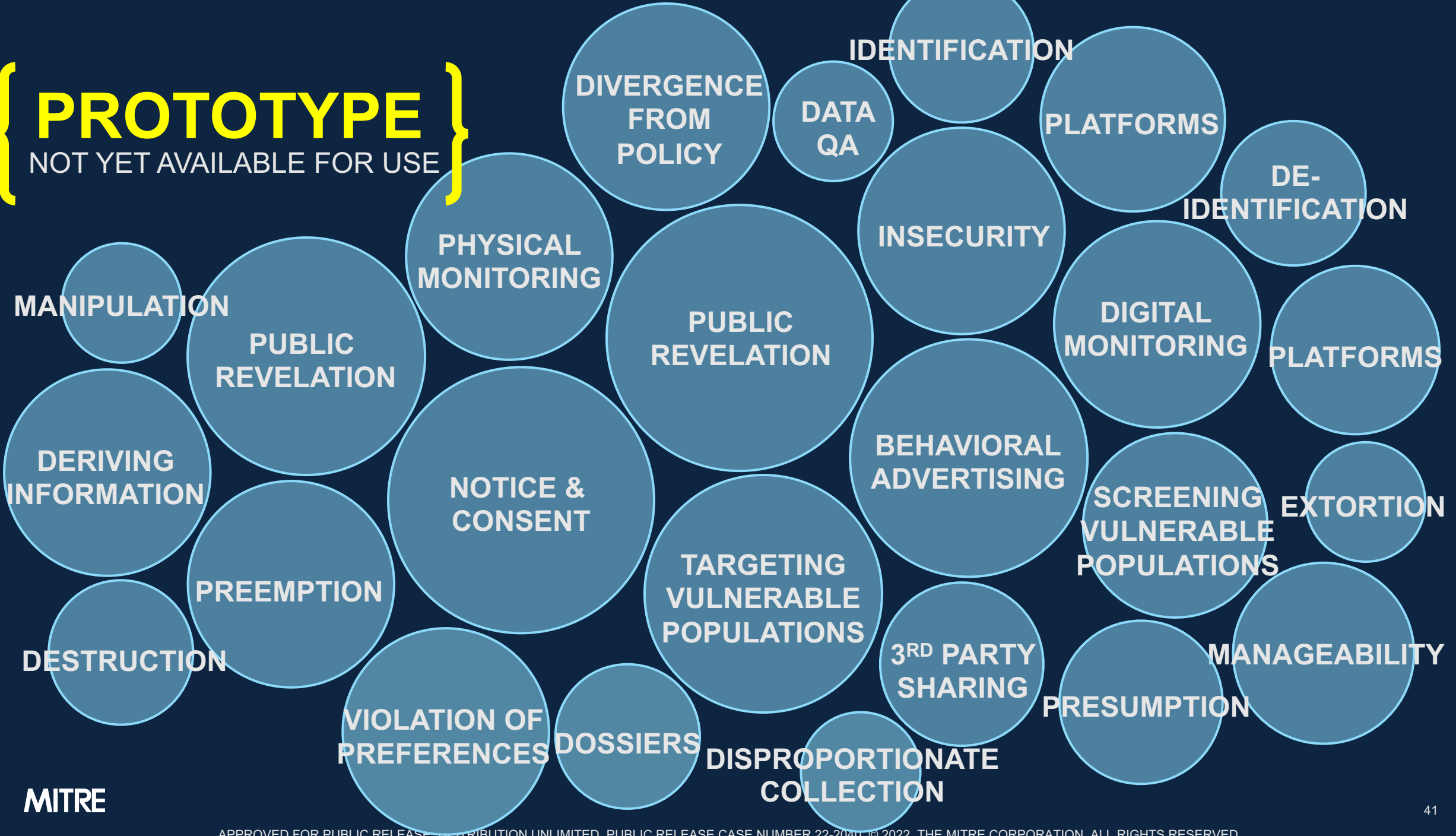
BACKUP

NOTICE	CONSENT	COLLECTION	INSECURITY	IDENTIFICATION	QUALITY ASSURANCE	MANAGEABILITY	AGGREGATION	PROCESSING	SHARING	USE	RETENTION & DESTRUCTION	DEVIATIONS
OUT OF SEQUENCE	OUT OF SEQUENCE	APPLICATION USE	LACK OF ACCESS CONTROLS	FINGERPRINT	AGE NOT VERIFIED	NO SUBJECT ACCESS	PII WITH OTHER DATA	BEHAVIORAL ANALYSIS	SHARING SENSITIVE DATA	IMPLICATE	DATA RETAINED AFTER USE	STATED POLICY
UNCLEAR	MISLEADING	REGISTRATION	INSUFFICIENT ENCRYPTION	TRACE	UNVETTED DATA SOURCE	NO SUBJECT MANAGEMENT	SENSITIVE DATA WITH OTHER DATA	TRAWLING FOR INFORMATION	SHARING DEROGATORY DATA	TARGET	DATA IMPROPERLY DESTROYED	DUA
MISLEADING	INSUFFICIENT	TRACKING	UNDERMINING AUTHENTICATION	RE-IDENTIFICATION	UNVETTED DATA ACCURACY	NO SUBJECT DELETION	MULTI-SOURCE AGGREGATION	INSUFFICIENT DOWNSTREAM REQUIREMENTS	UNANTICIPATED SHARING	EXTORT		CLAIMED CERTIFICATION
INSUFFICIENT	ABSENT	SNIFFING	DETECTION FAILURE	PERSISTENT IDENTIFIER	UNVETTED RECIPIENT	SETTINGS AFFECTED BY OUTSIDE FORCES	PROFILING	INTERNAL APPROPRIATION	UNANTICIPATED PUBLISHING	MANIPULATE		REGULATION
ABSENT	NO OVERALL OPT OUT	PRETEXTING	INSUFFICIENT DOWNSTREAM REQUIREMENTS		UNVETTED SECURITY	CONFOUNDED USER CONTROLS		INTRODUCING BIAS	EXPOSURE	INTRUDE		
INCORRECT	NO GRANULAR OPT OUT	EXTERNAL APPROPRIATION	MISCONFIGURED PERMISSIONS		UNEVALUATED DATA BIAS	BYPASS		CLUSTERING	DOXXING	TAILORED DISPLAY		
	INHERITED	INTERCEPTION			DATA NOT DE-IDENTIFICATION	PREEMPTION OF SETTINGS		INSUFFICIENT DE-IDENTIFICATION	INSUFFICIENT CONTEXT	SELL		
		SOLICITING						INDESCRIMINATE PROCESSING	INSUFFICIENT DUA			
		RECORDING						DERIVING DEROGATORY INFORMATION	RECIPIENTS ACTING OUTSIDE DUA			
		DATA GENERATION						DERIVING SENSITIVE INFORMATION	NO RESTRICTIONS ON USE			
								INFERRING ABOUT SENSITIVE POPULATIONS	AFFORDING REVELATIONS			

PROTOTYPE
 NOT YET AVAILABLE FOR USE

{ PROTOTYPE }

NOT YET AVAILABLE FOR USE



SOCIO-TECHNICAL CONTEXT

- Information outside the attack killchain that informs the threat level

ENVIRONMENT	INTERACTION	ENGAGEMENT	DISTRIBUTION	DATA TYPE
DIGITAL	NONE	SENSITIVE POPULATIONS	ONE TO ONE	IDENTIFIER
PHYSICAL	SINGLE POINT	SPECIFIC INDIVIDUALS	ONE TO MANY	CREDENTIALS
	MULTI POINT	BIASED SAMPLE	ONE TO EVERYONE	CONTACT
	CONTINUOUS			DEMOGRAPHIC
				HEALTH
				FINANCIAL
				BIOMETRIC
				BEHAVIOR
				LOCATION
				IMAGES, VIDEO, VOICE
				SOCIAL MEDIA