Bridging the Gap between Privacy Incidents and PETs

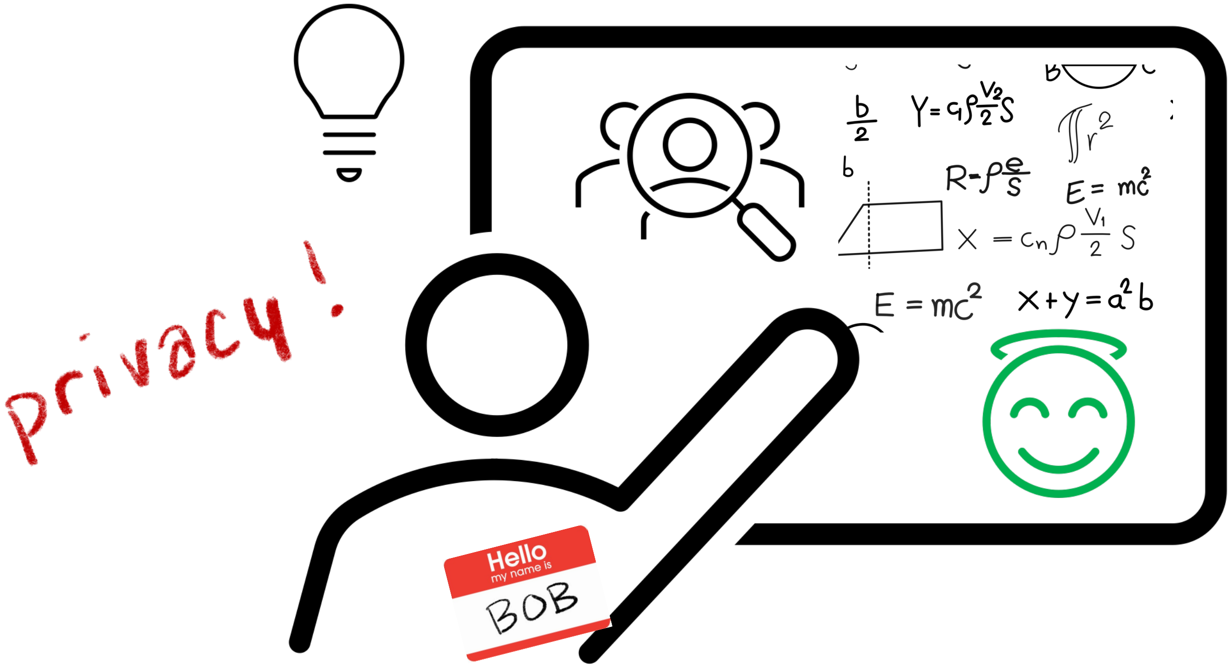
Shannon Veitch, Lena Csomor, Alexander Viand, Anwar Hithnawi, Bailey Kacsmar

ETH zürich

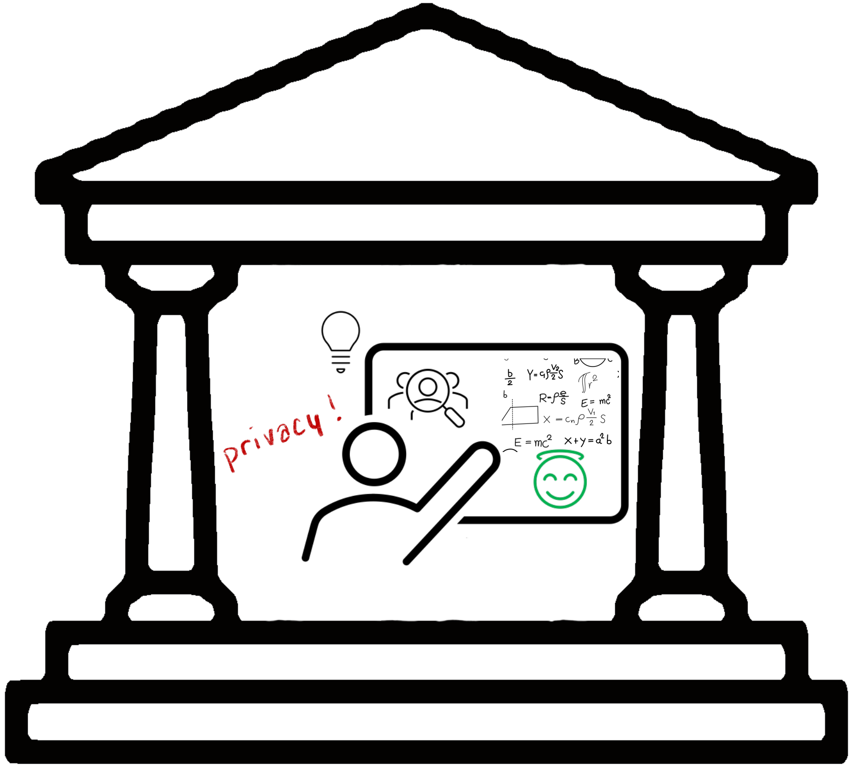
UNIVERSITY OF ALBERTA

Development of Privacy Enhancing Technologies (PETs)

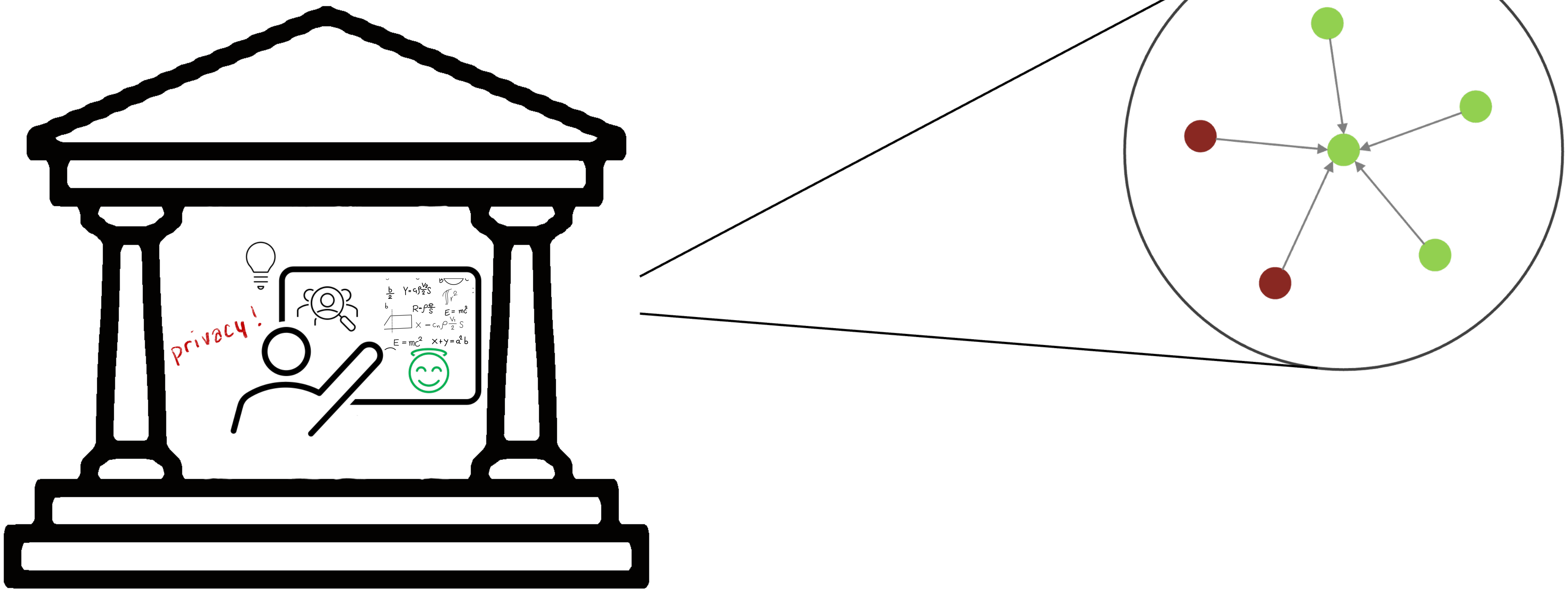
Development of Privacy Enhancing Technologies (PETs)



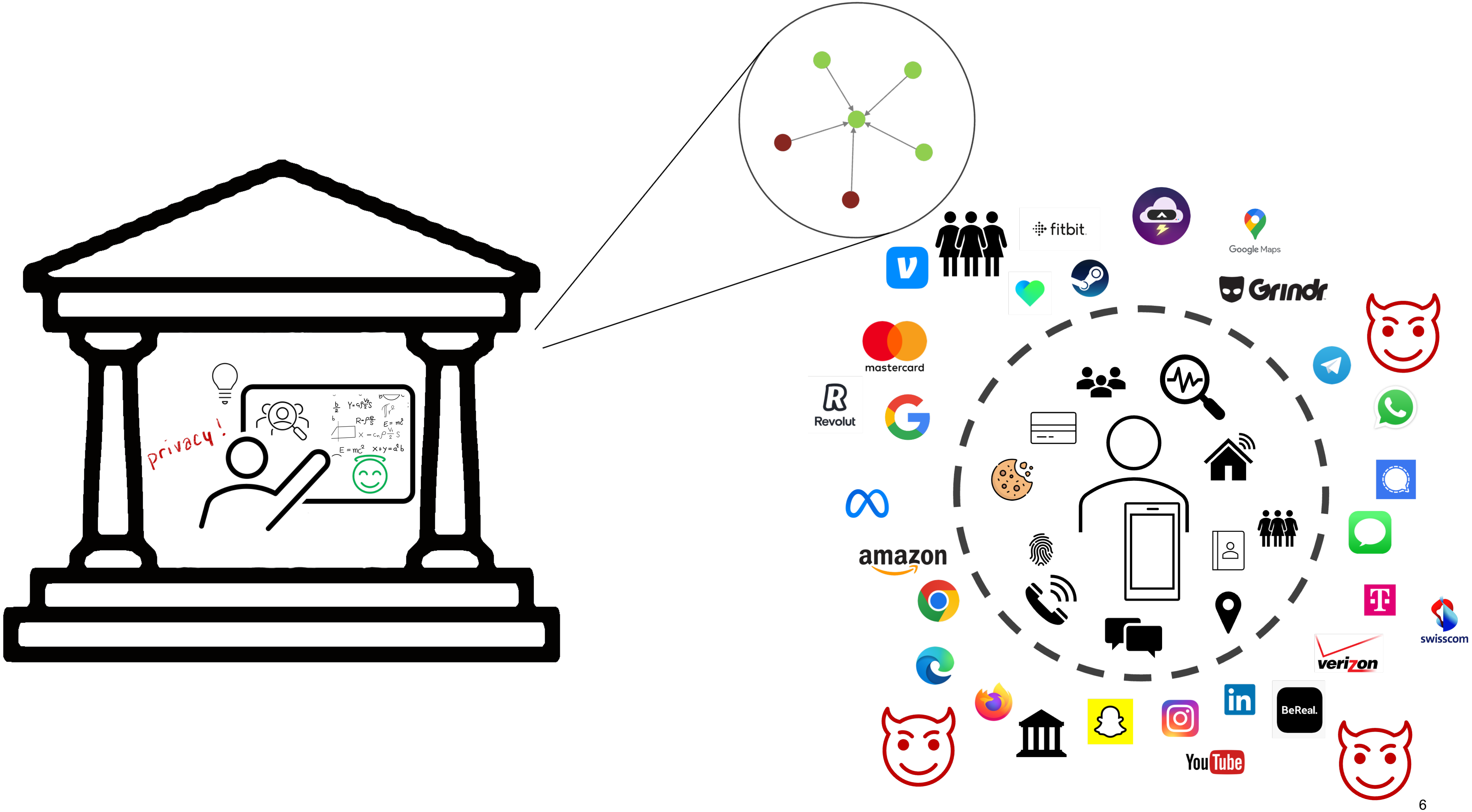
Development of Privacy Enhancing Technologies (PETs)



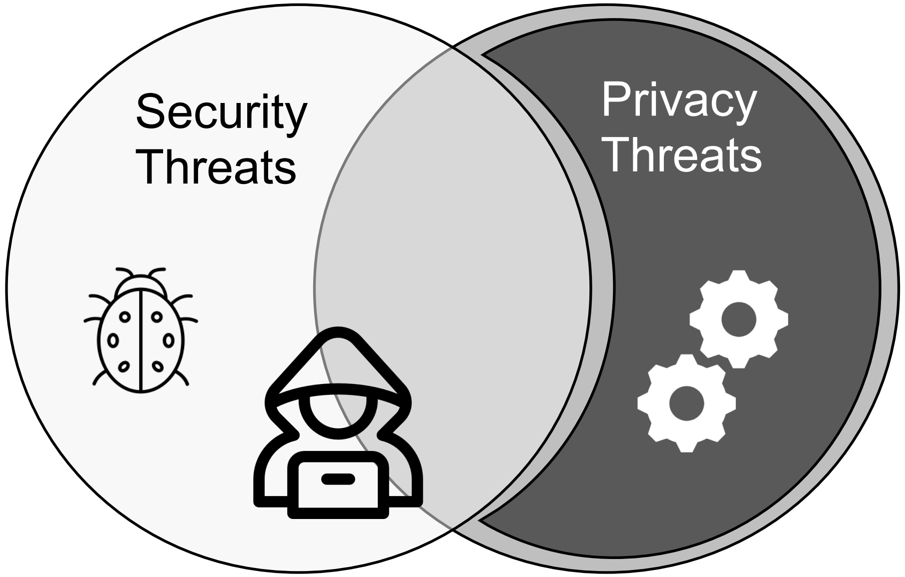
Development of Privacy Enhancing Technologies (PETs)



Development of Privacy Enhancing Technologies (PETs)



Scope

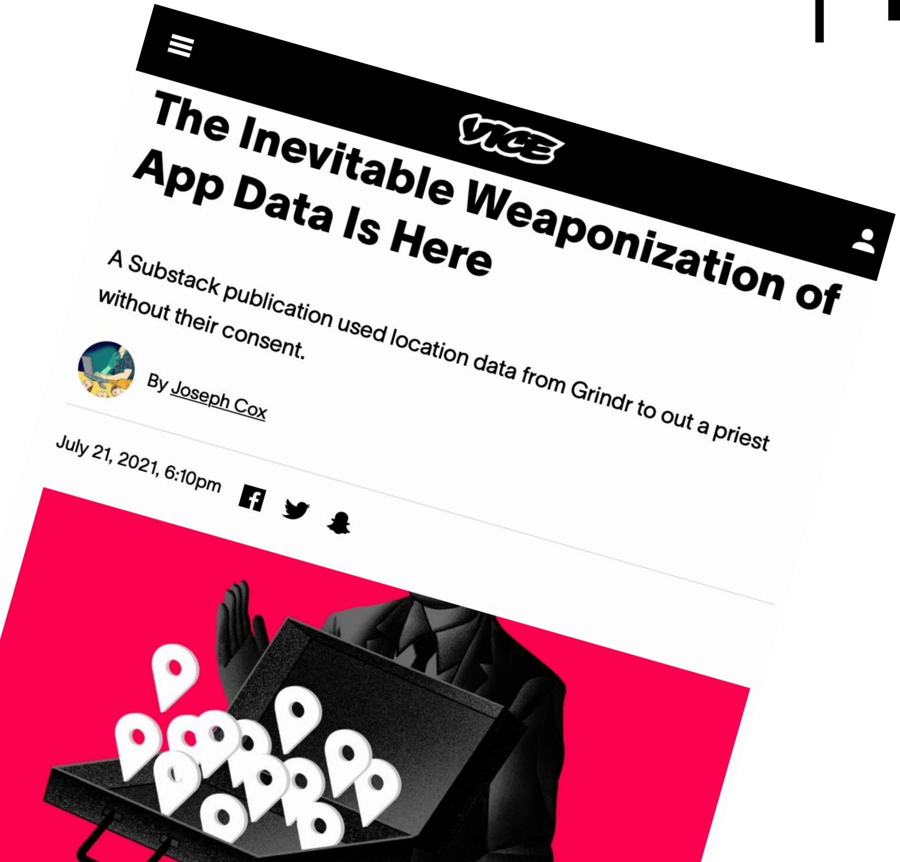


Westin's Definition of Privacy (1967)

An entity's **ability to control** how, when, and to what extent personal information about it is communicated to others

We are interested in the **harms** (consequences) caused by privacy violations.

Threat Models in Real Life?



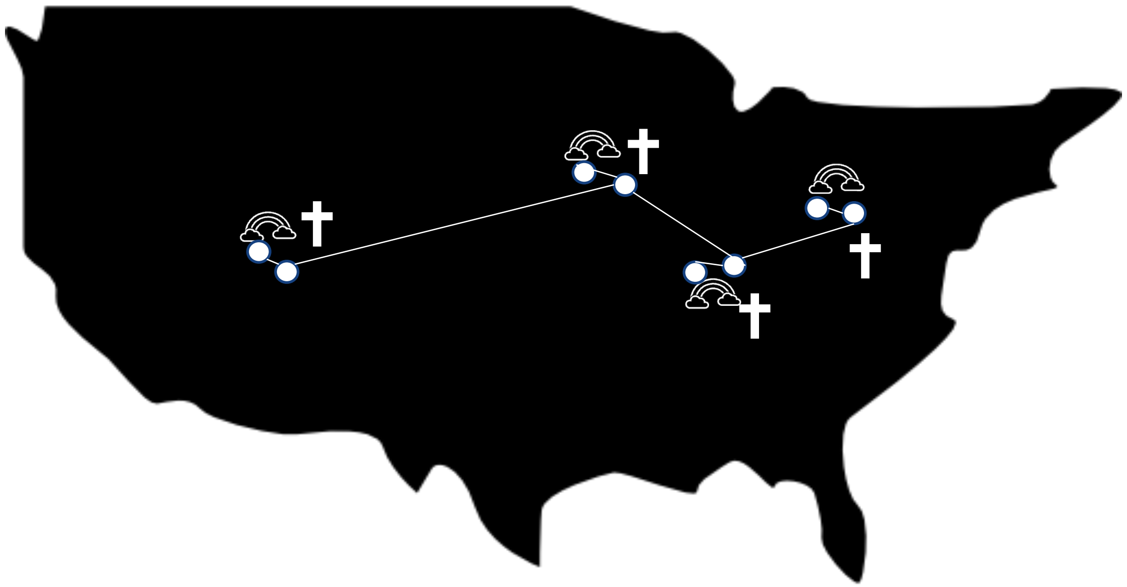
VICE

The Inevitable Weaponization of App Data Is Here

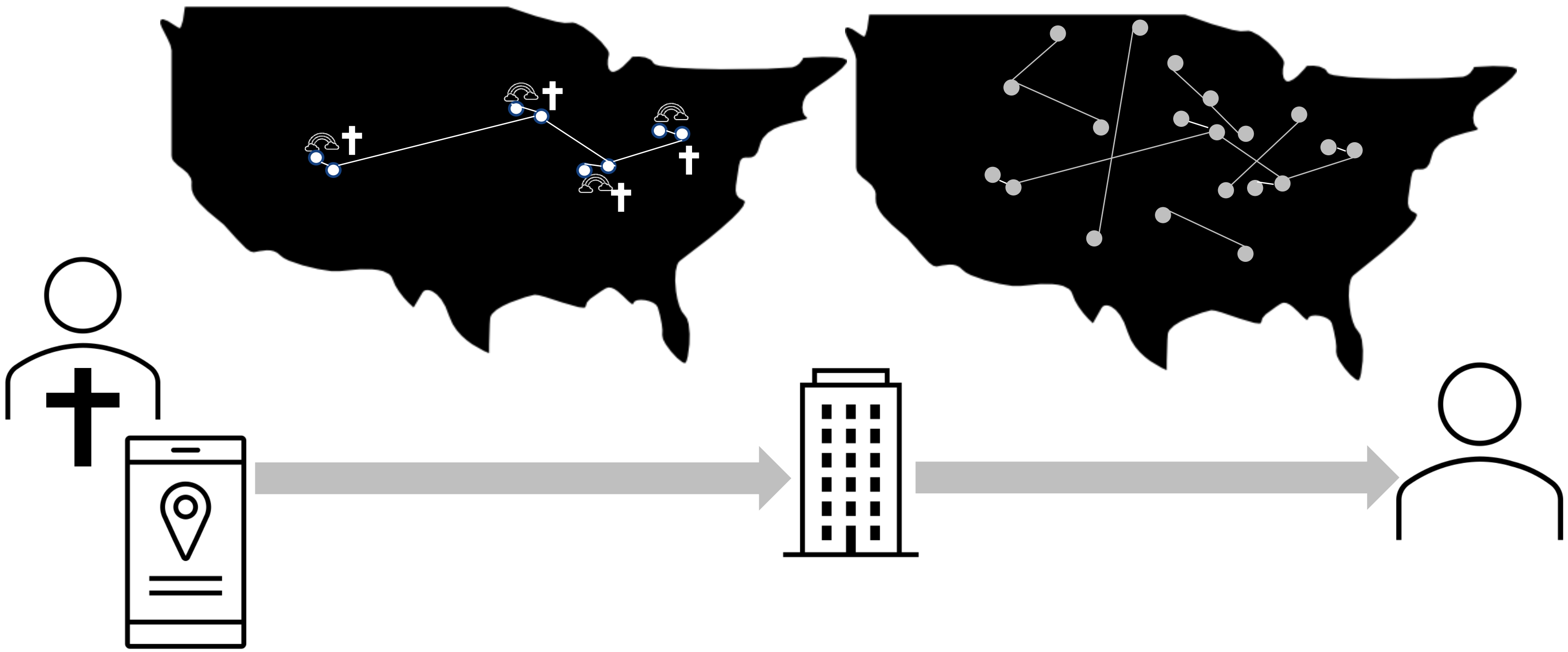
A Substack publication used location data from Grindr to out a priest without their consent.

By Joseph Cox

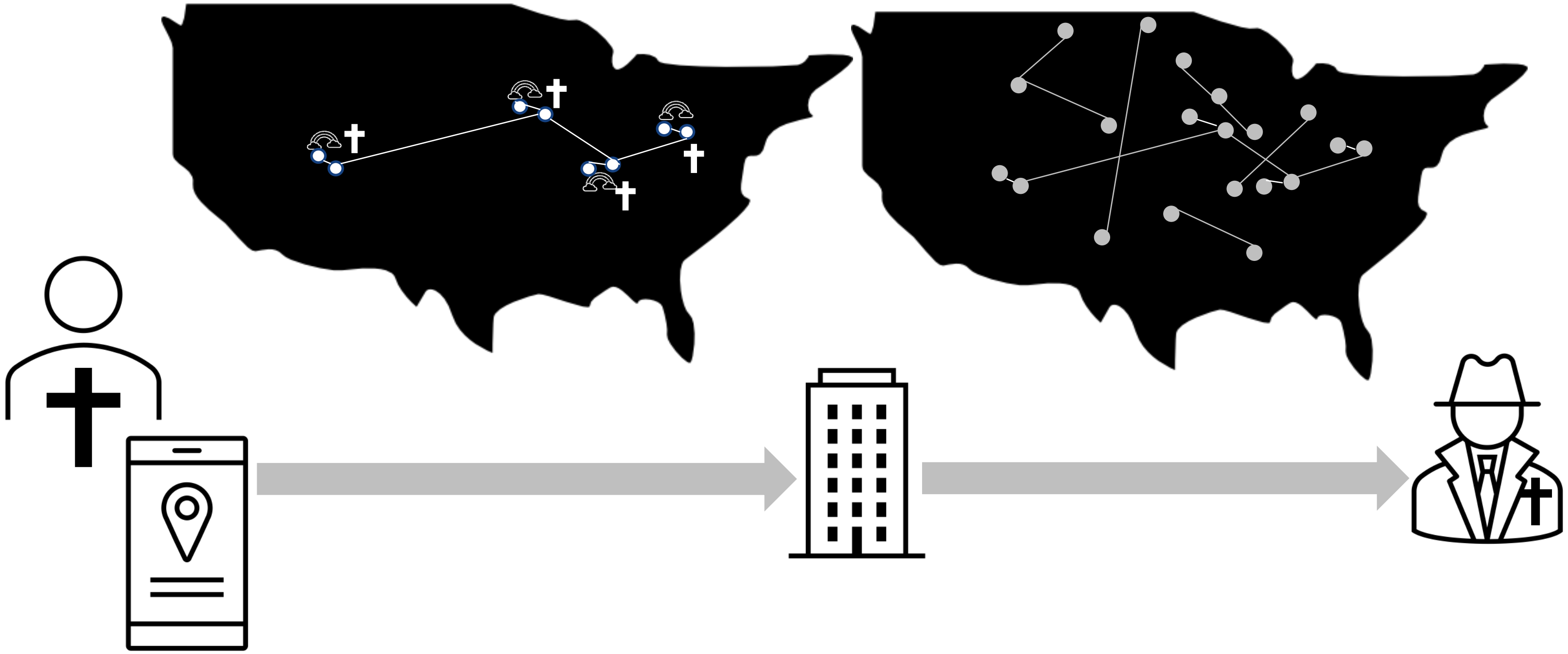
July 21, 2021, 6:10pm



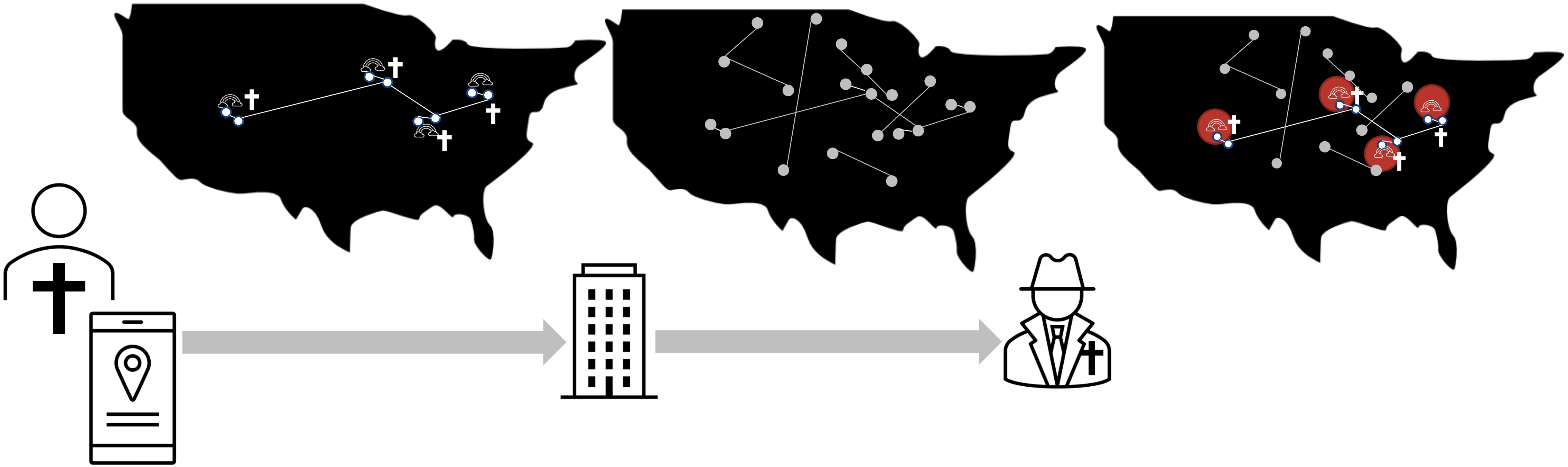
Threat Models in Real Life?



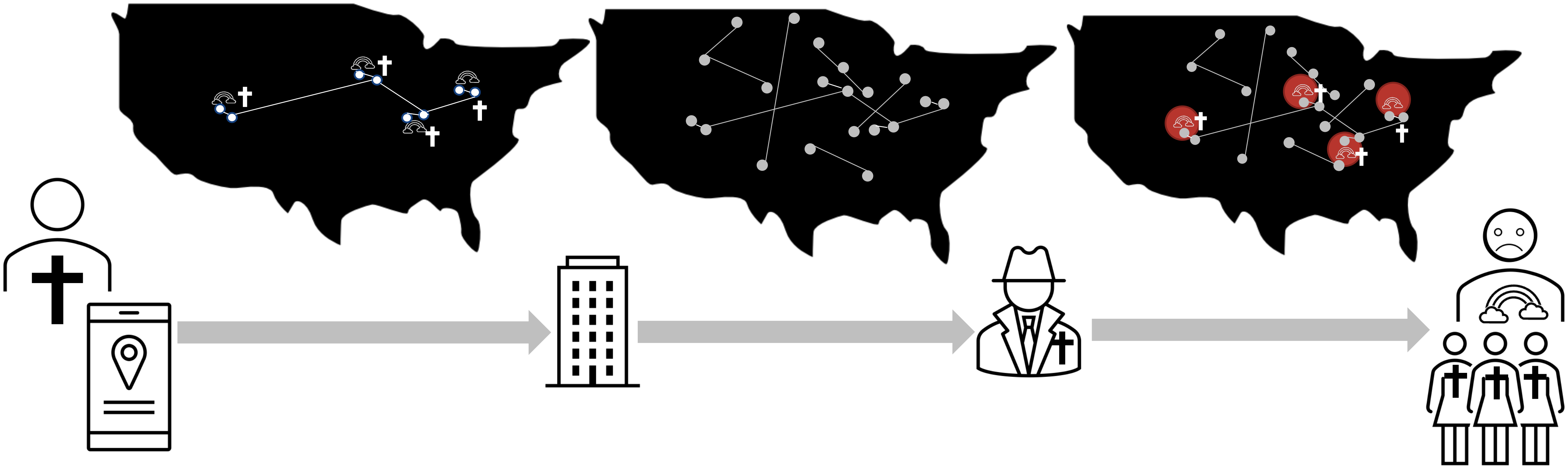
Threat Models in Real Life?



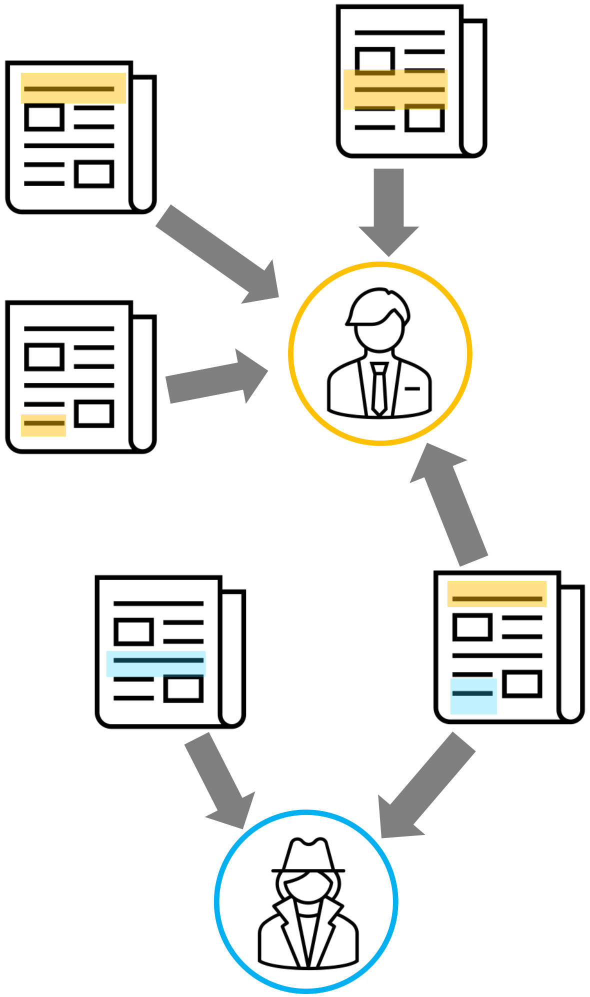
Threat Models in Real Life?



Threat Models in Real Life?

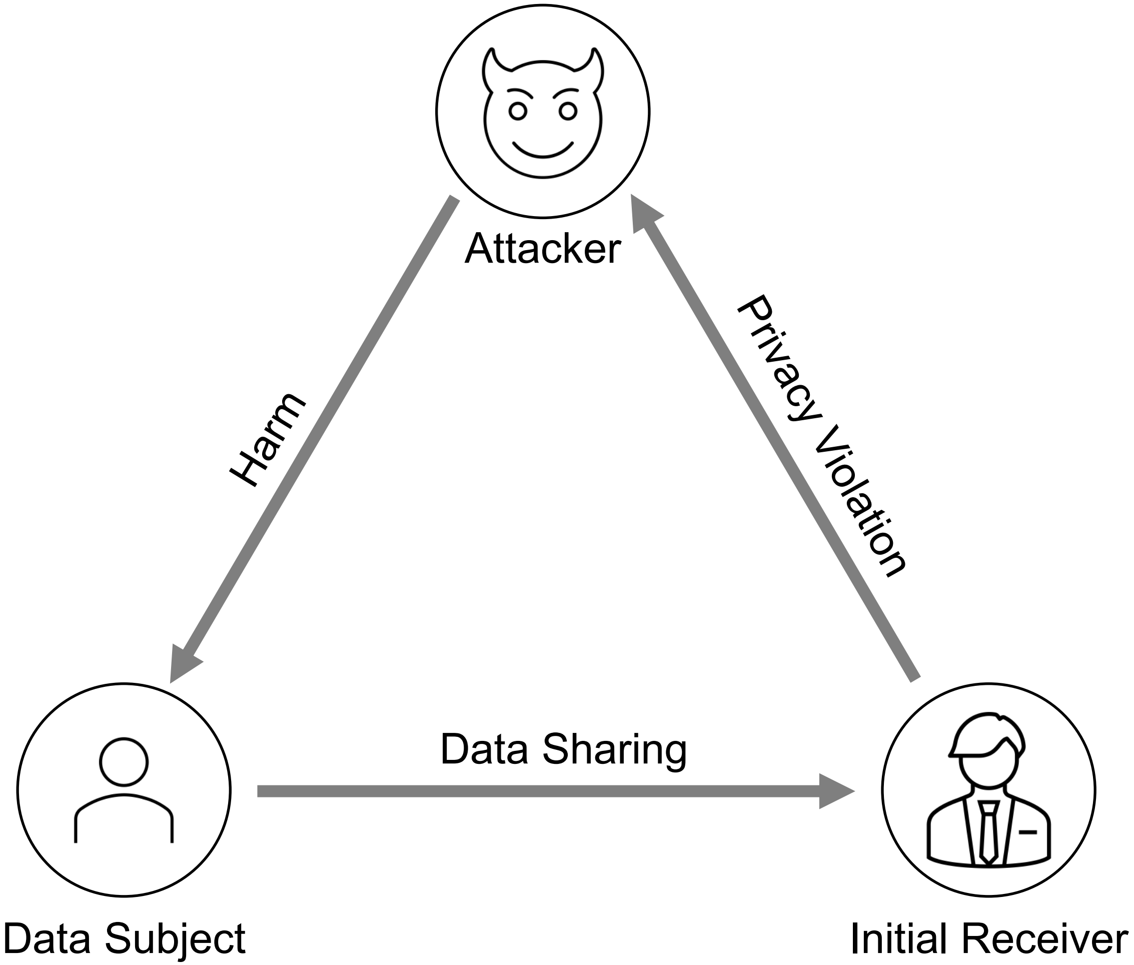


Analysis of Past Privacy Incidents

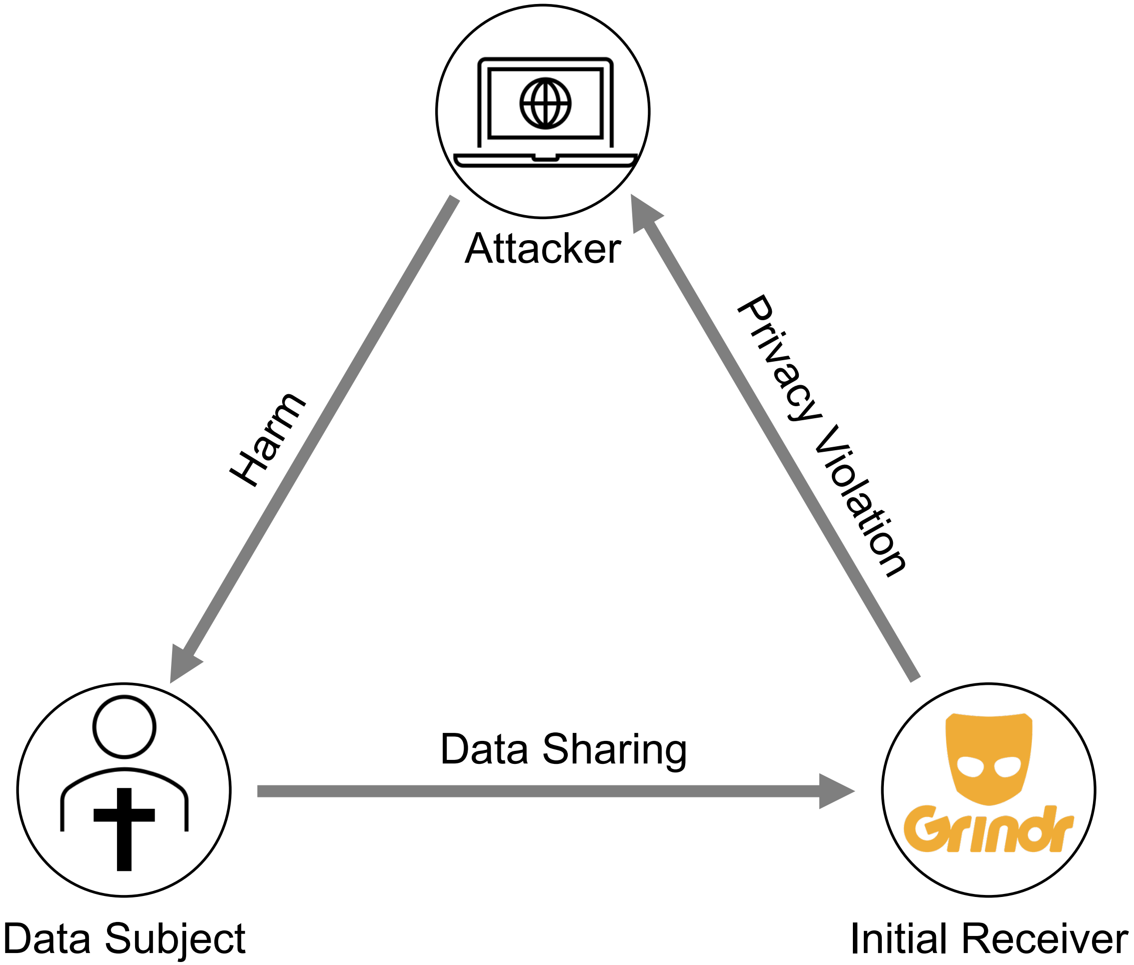


- Over 100 articles: The New York Times VICE
- Privacy-based Attack Model
- Inductive Collection of Context

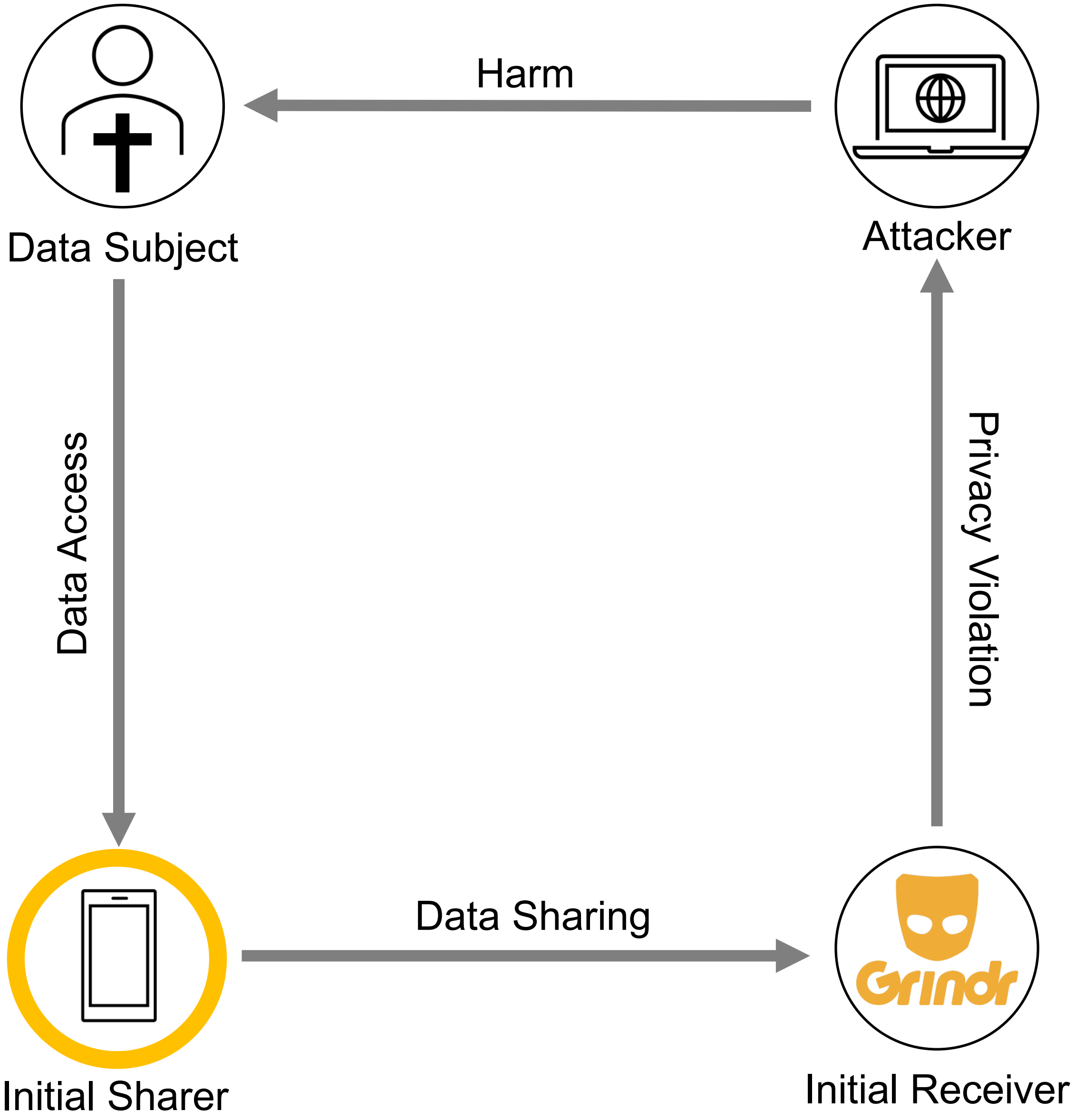
Defining a Privacy-based Attack



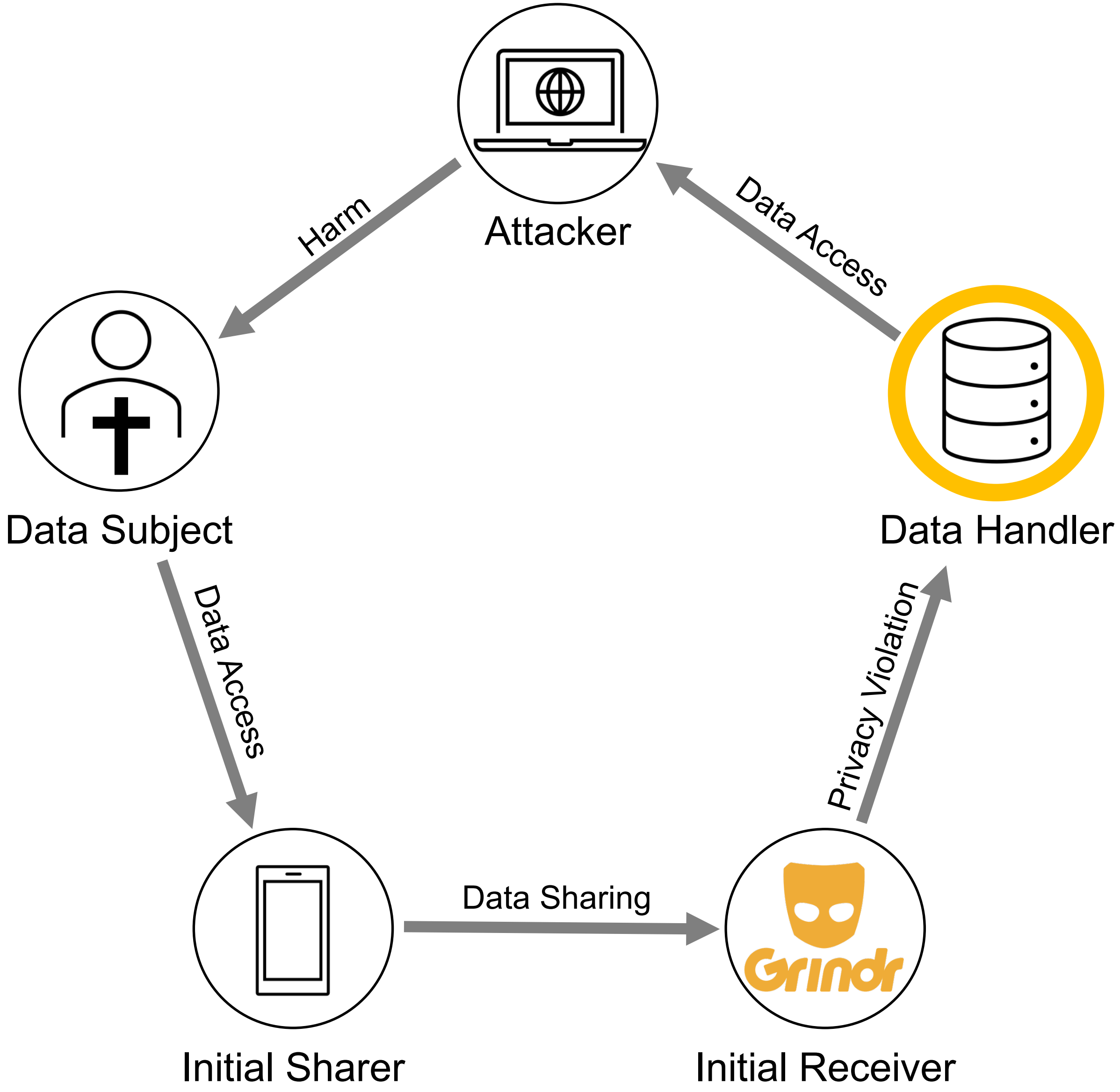
Defining a Privacy-based Attack



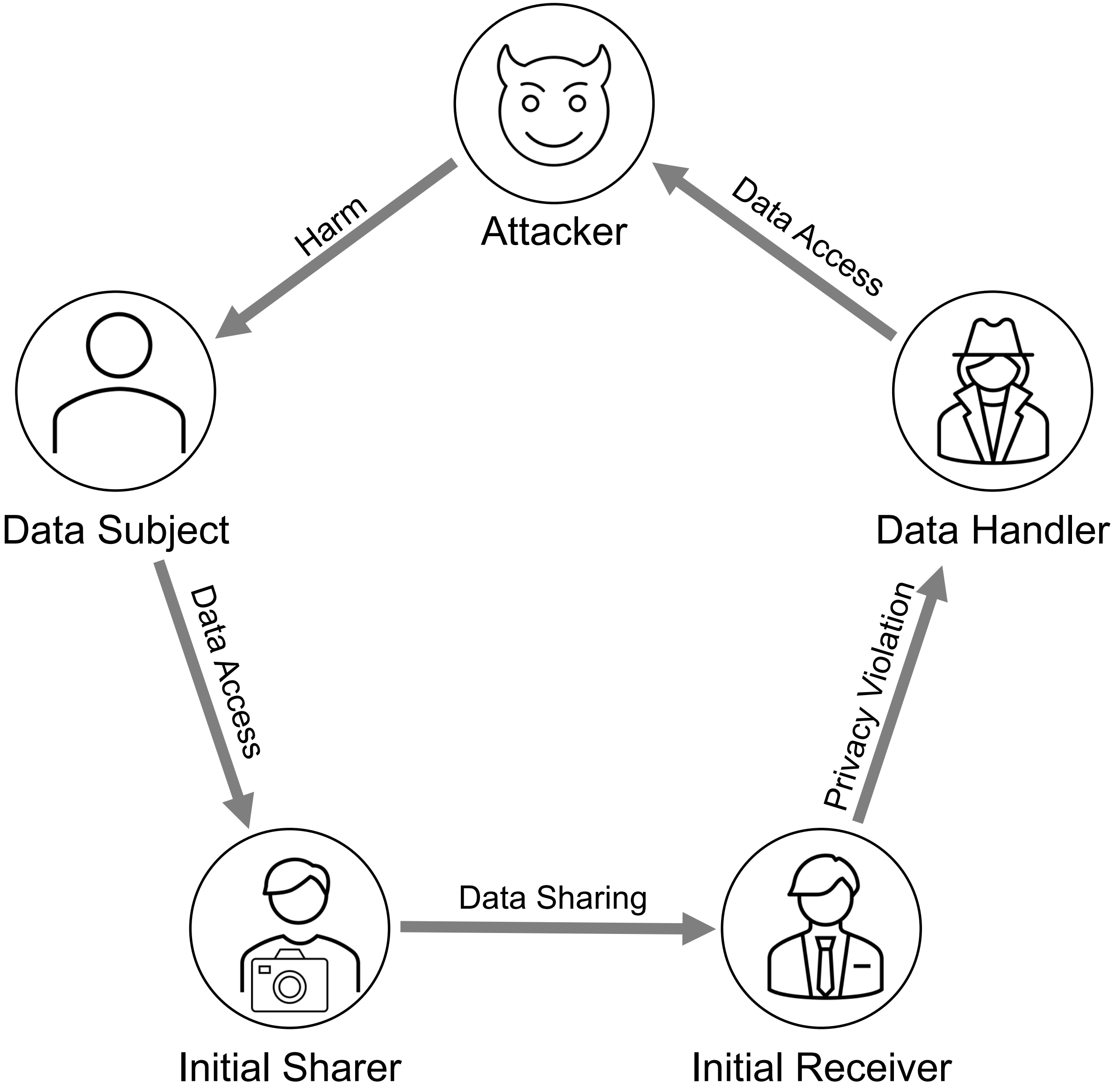
Defining a Privacy-based Attack



Defining a Privacy-based Attack



Defining a Privacy-based Attack

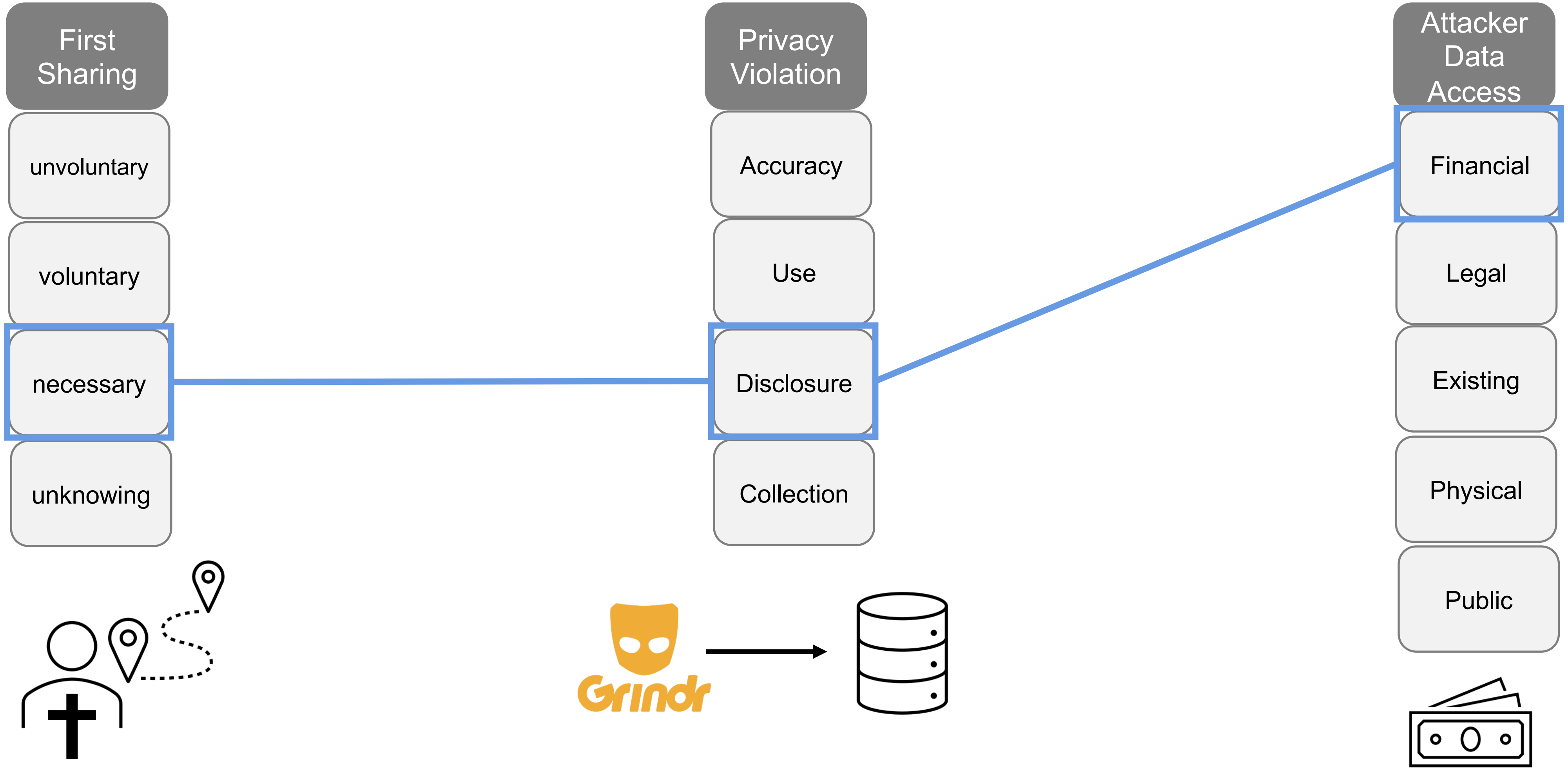


Data Subject	Initial Sharer	Data Sharing →	Initial Receiver	Privacy Violation →	Data Handler	Data Access →	Attacker	Harm →
Public Person	Stranger	unvoluntary	Stranger	Accuracy	Stranger	Financial	Stranger	Financial
Common Person	Personal Connection	voluntary	Personal Connection	Use	Personal Connection	Legal	Personal Connection	Social
	Gov	necessary	Gov	Disclosure	Gov	Existing	Gov	Mental
	Company	unknowing	Company	Collection	Company	Physical	Company	physical
	Self					Public		Legal Prosecution
								Mass Surveillance
								Targeted Ads

Analysis of Past Privacy Incidents

ctim havior	Data Subject	Initial Sharer	First Sharing	Initial Receiver	Privacy Violation	Data Handler	Attacker Data Access	Attacker	Harm	Target	Data Type	Attacke Motivati
oversial ions	Public Person	Personal Connection	unvoluntary	Personal Connection	Accuracy	Personal Connection	Financial	Personal Connection	Financial	targeted	Visual Data	financ
rmal nline	Common Person	Stranger	voluntary	Stranger	Use	Stranger	Legal	Stranger	Social	untargeted	Behavior	intentio
rmal ffline		Gov	necessary	Gov	Disclosure	Gov	Existing	Gov	Mental	filtered	Biometric Data	collate
liance law ement		Company	unknowing	Company	Collection	Company	Physical	Company	physical		DNA	
		Self				Same as IR	Public	Same as IR	Legal Prosecution		Messages	
								Same as DH	Mass Surveillance		Personal Info	
									Targeted Ads		Location	
											Medical	

Analysis of Past Privacy Incidents

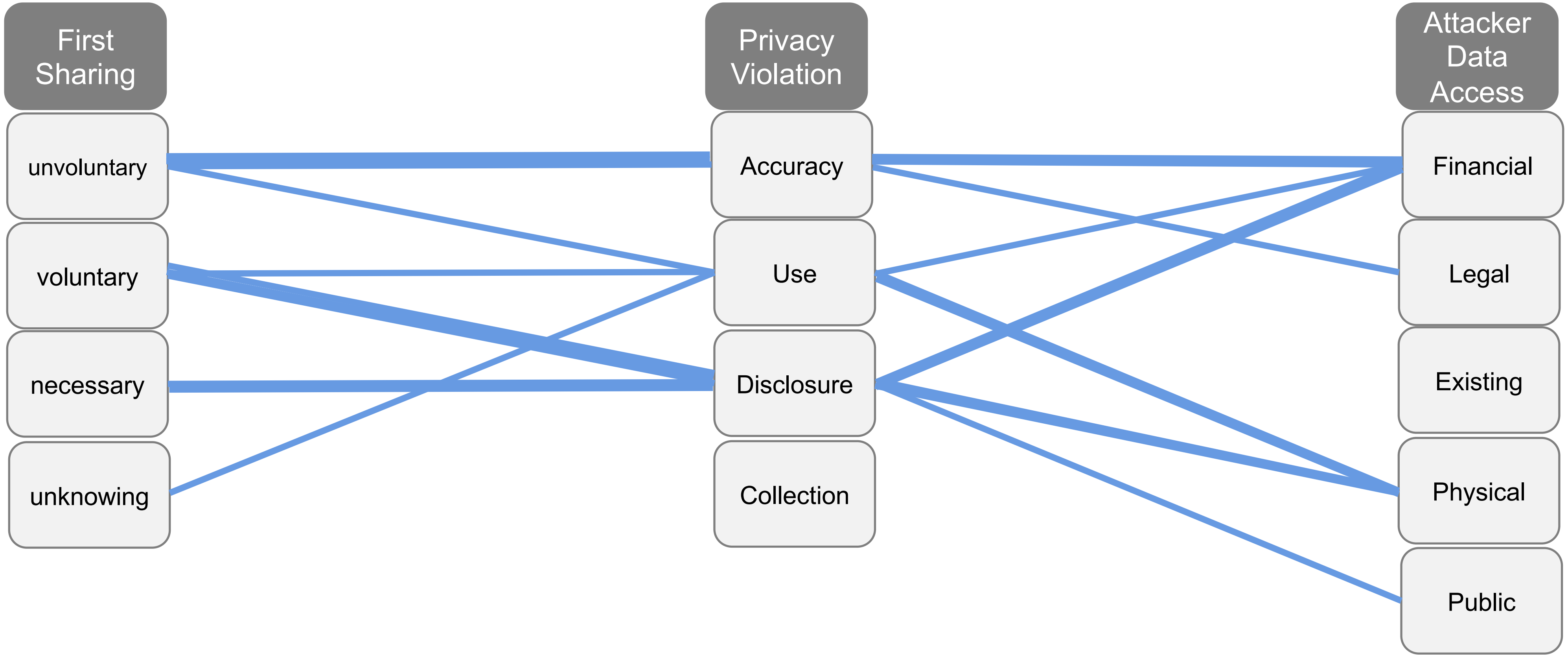


First Sharing
- unvoluntary
- voluntary
- necessary
- unknowing

Privacy Violation
- Accuracy
- Use
- Disclosure
- Collection

Attacker Data Access
- Financial
- Legal
- Existing
- Physical
- Public

Analysis of Past Privacy Incidents



First Sharing

unvoluntary

voluntary

necessary

unknowing

Privacy Violation

Accuracy

Use

Disclosure

Collection

Attacker Data Access

Financial

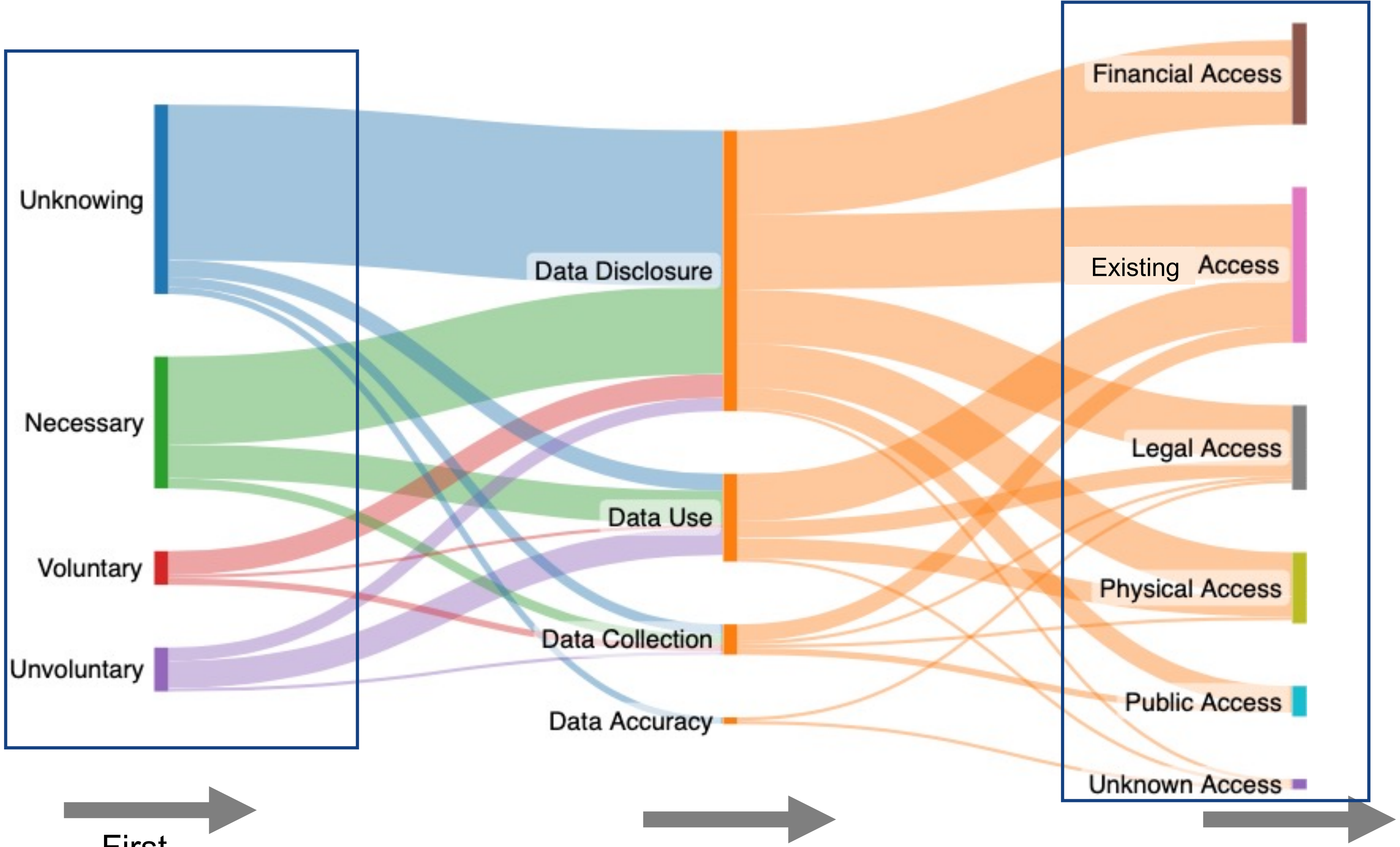
Legal

Existing

Physical

Public

Analysis of Past Privacy Incidents

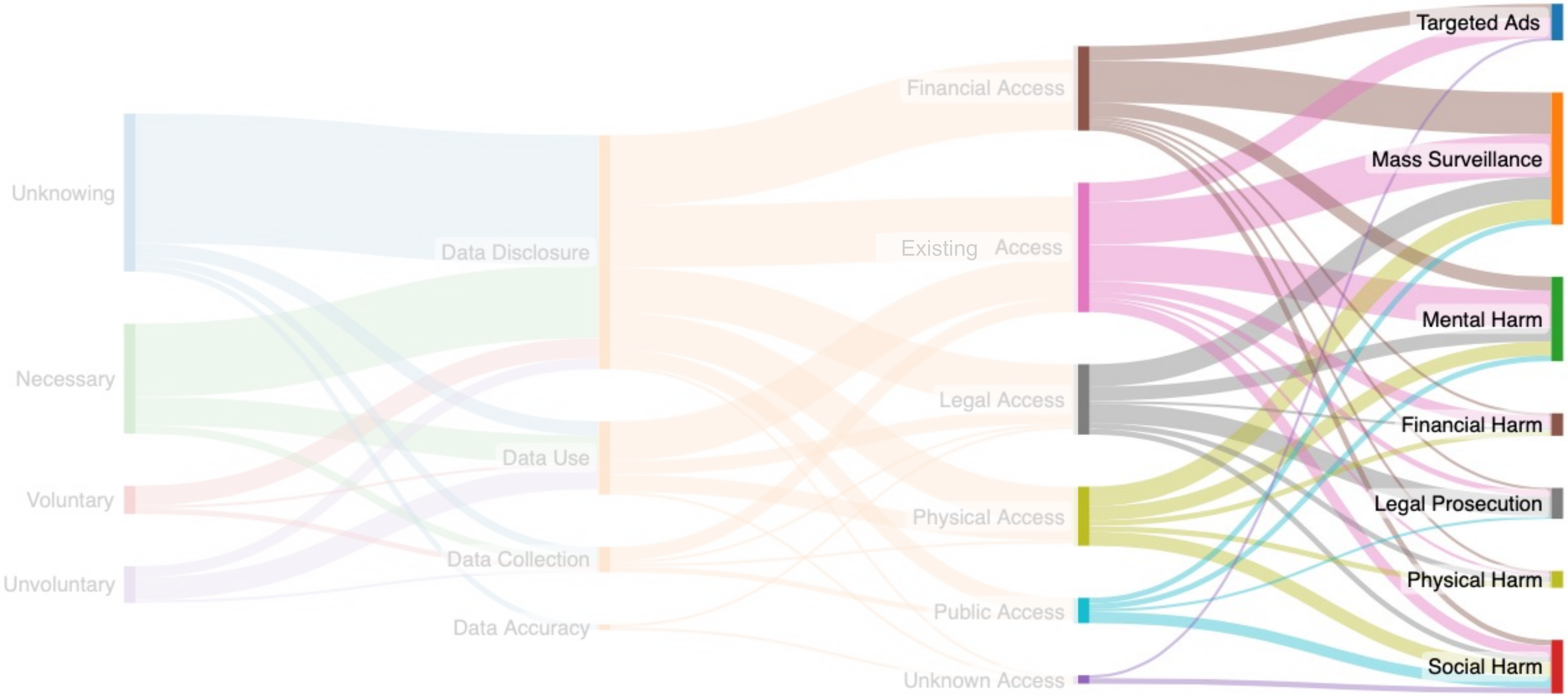


First Sharing

Privacy Violation

Attacker Data Access

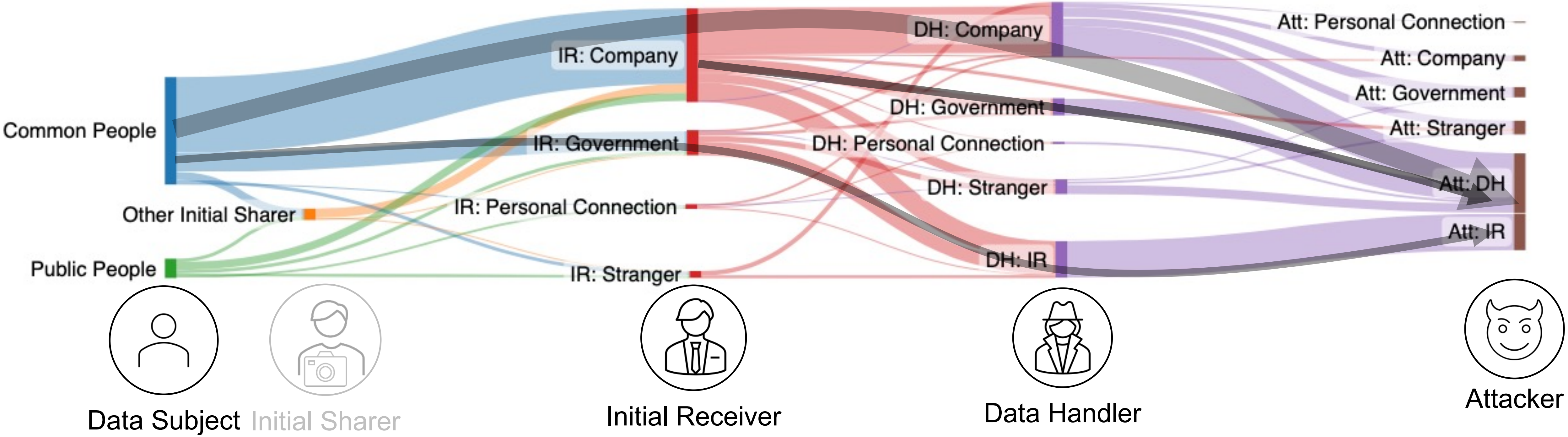
Against which **consequences of privacy violations** might a user require protection?



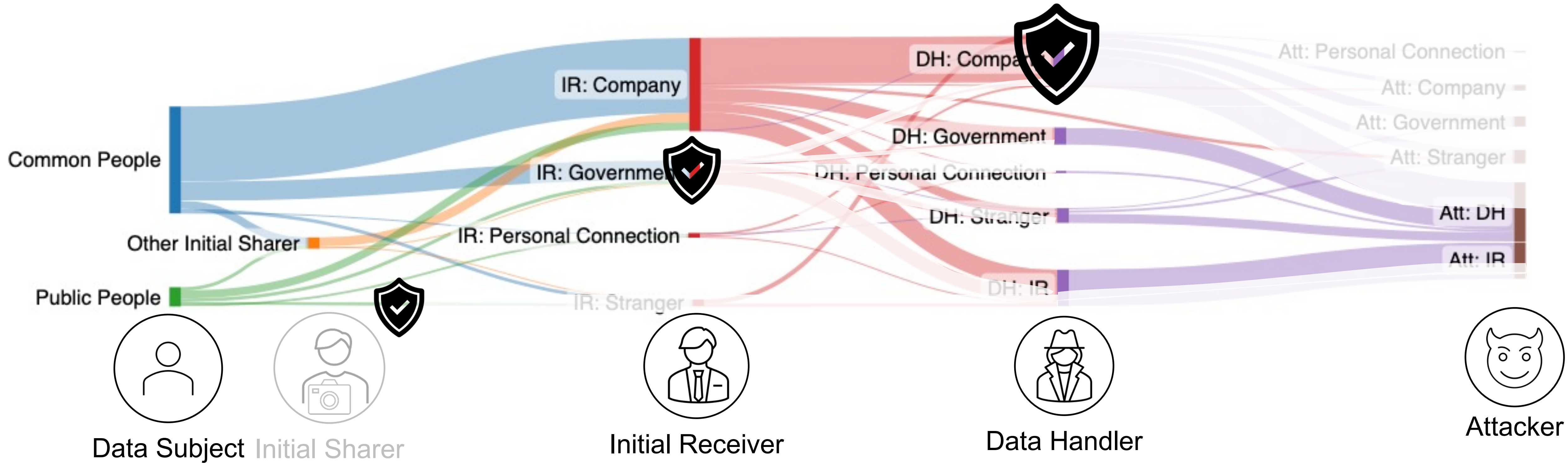
Analysis of Past Privacy Incidents

ctim avior	Data Subject	Initial Sharer	First Sharing	Initial Receiver	Privacy Violation	Data Handler	Attacker Data Access	Attacker	Harm	Target	Data Type	Attacke Motivati
oversial ions	Public Person	Stranger	unvoluntary	Stranger	Accuracy	Stranger	Financial	Stranger	Financial	targeted	Visual Data	financ
rmal nline	Common Person	Personal Connection	voluntary	Personal Connection	Use	Personal Connection	Legal	Personal Connection	Social	untargeted	Behavior	intentio
rmal fline		Gov	necessary	Gov	Disclosure	Gov	Existing	Gov	Mental	filtered	Biometric Data	collate
liance law ement		Company	unknowing	Company	Collection	Company	Physical	Company	physical		DNA	
		Self				Same as IR	Public	Same as IR	Legal Prosecution		Messages	
								Same as DH	Mass Surveillance		Location	
									Targeted Ads			

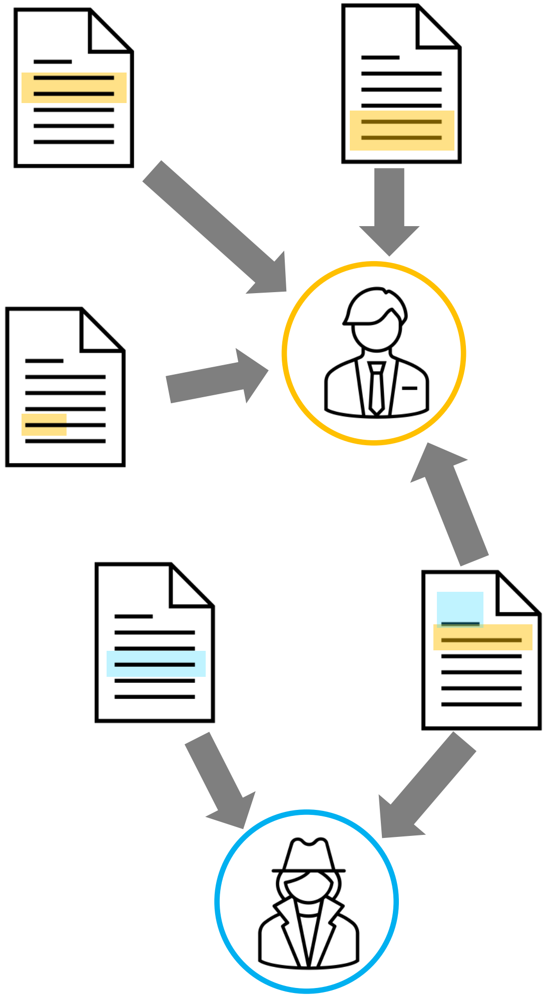
Analysis of Past Privacy Incidents



Impact of PETs?



Analysis of PETs in the Literature



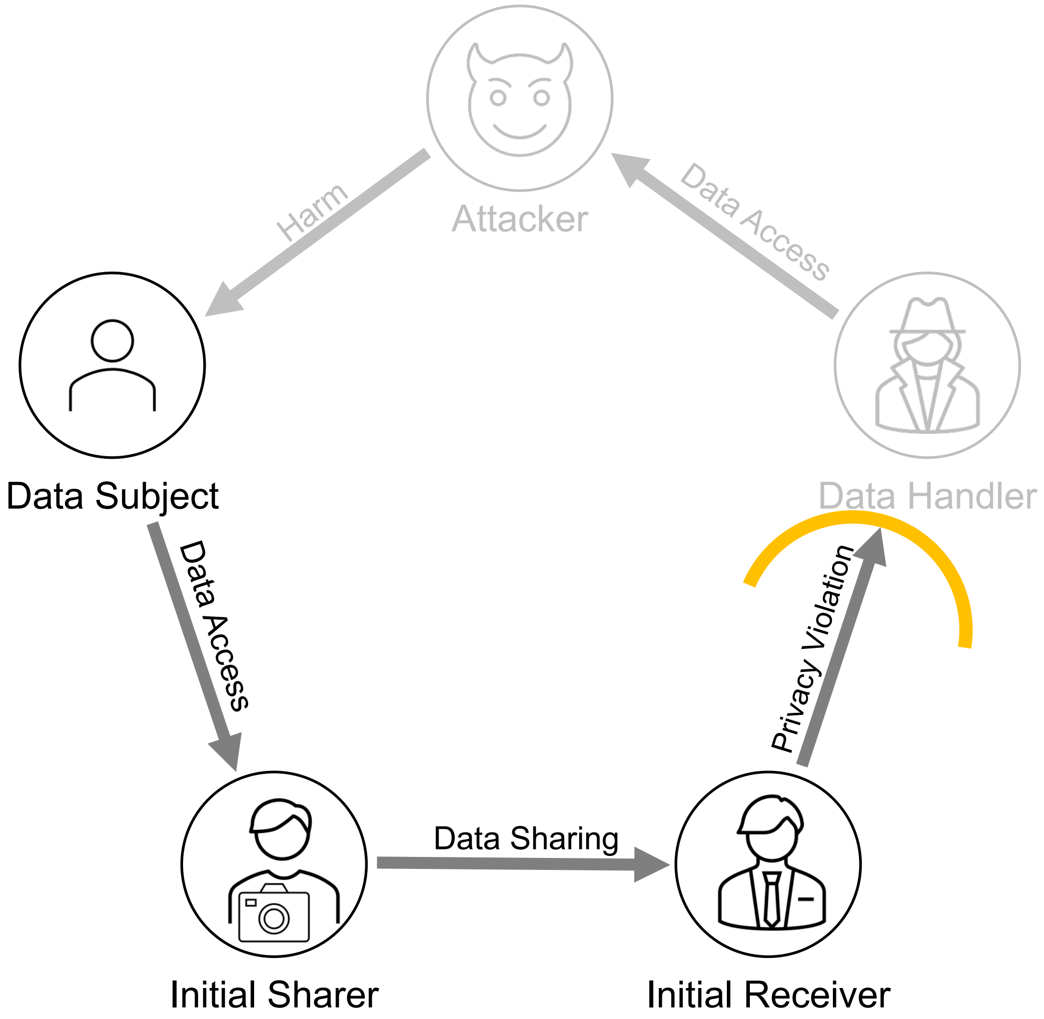
Focus on Alteration of Data Flow & Control

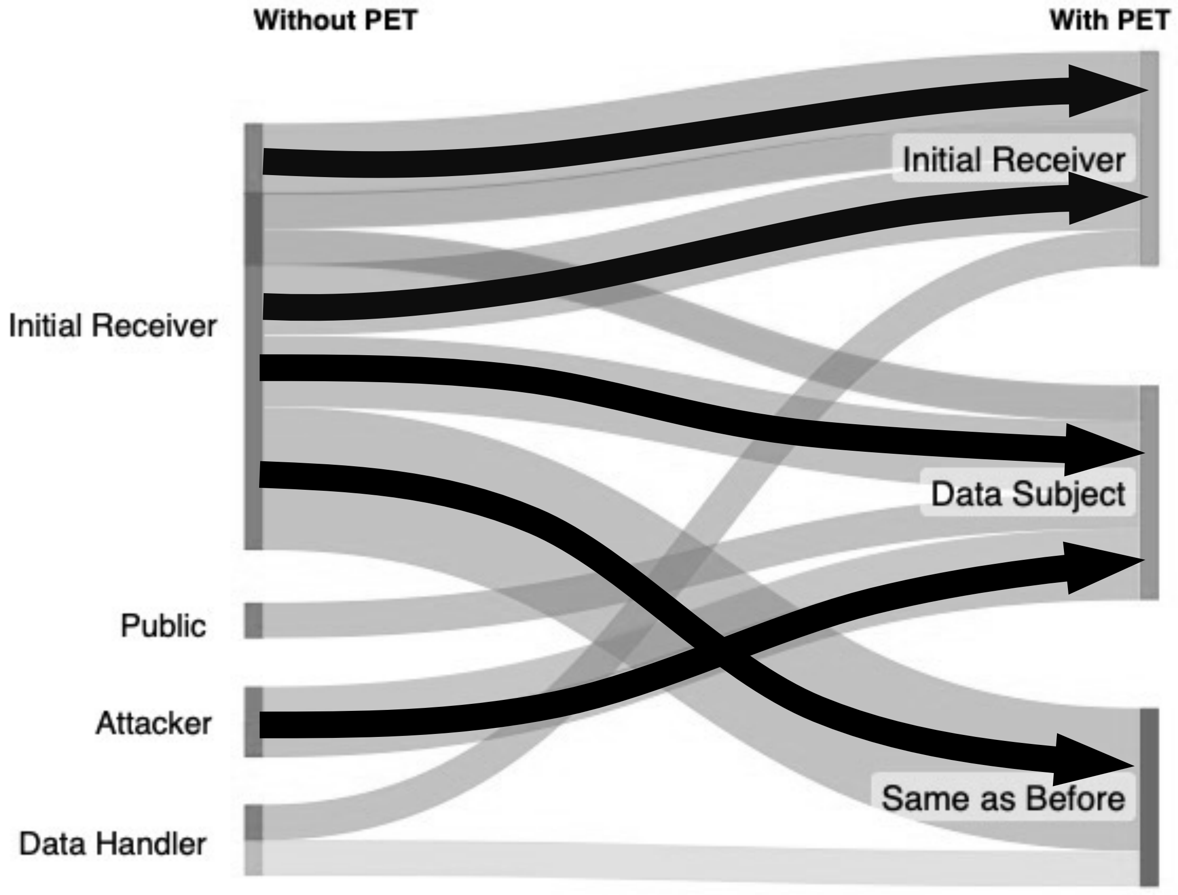
Compare to Real-World Attacks

Papers with Usenix Test of Time or Caspar Bowden Award

N = 103. 17 of which proposed new PETs with real-life privacy scenarios

Shift of Control



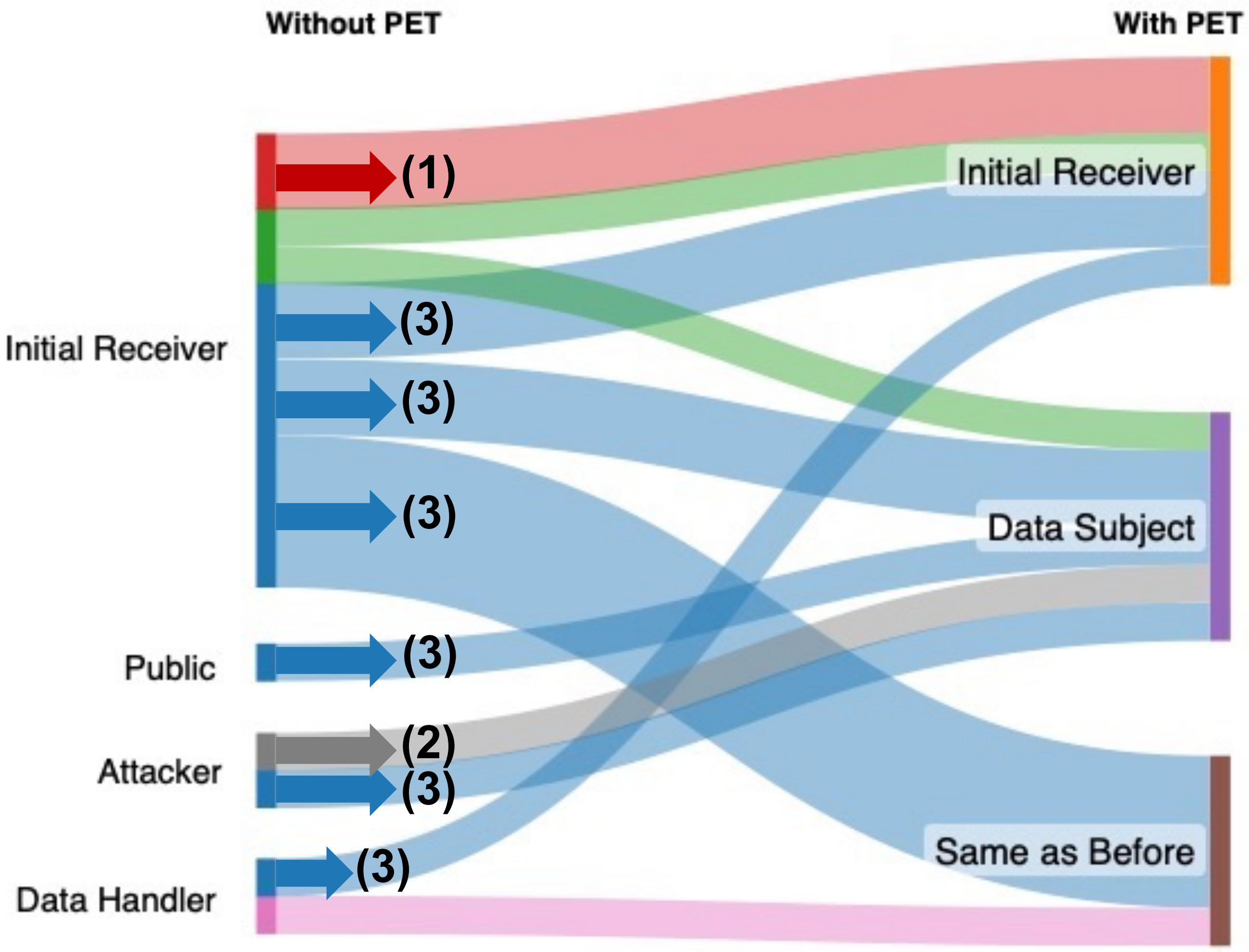


Alterations to the Data Flow

(1) Added flows

(2) Intercepted flows

(3) Narrowed flows



Discussion

Threat Modelling: Simple models which allow for analysis are at odds with the complexities of real-life data flows. *How can we capture the complexity of real-world systems in PETs development?*

Privacy Harms: *Are PETs more focused on protecting assets than avoiding consequences?* Focusing on harms caused to users provides new perspectives on trade-offs and trust.

The Role of PETs: Existing PETs are sometimes **adding** data flows (as opposed to intercepting them). *Is this behaviour truly enhancing privacy?*