Assessing Privacy Risk with the IPA Triad

Mark Funk

Hi, I’m Mark.

Pronouns: they / them

Hi, I’m Mark.

Pronouns: they / them

Advisor, Breaker, Defender, Builder, and Designer.

Hi, I’m Mark.

Pronouns: they / them

Advisor, Breaker, Defender, Builder, and Designer.

Priors: Consulting, Google, Square, misc startups

01 INTRODUCTION

Context clues.

02 THE PROPERTIES

What are they? Examples and implications.

03 RISK ASSESSMENT

Abstract use case for privacy properties.

04 USE CASES

Specific applications. Observed outcomes.

01

Introduction

What does it even mean to be “Private” anyways?

Let’s borrow from our peers in security

Let’s borrow from our peers in security

The CIA Triad

- Confidentiality
- Integrity
- Availability

Information Security defends against attackers, who would seek to subvert one (or more) of the above properties to achieve their goals.

Existing Approaches

Existing Approaches

Legal Definition!

Existing Approaches

Legal Definition!

User Perspective!

Existing Approaches

Legal Definition!

User Perspective!

Threat Actors!

The IPA Triad

The IPA Triad

Identity

The IPA Triad

Identity

Presence

The IPA Triad

Identity

Presence

Activity

02

The Properties

Identity, Presence, and Activity

Identity

Describes **data which reveals who** an individual, group, or population **is**.

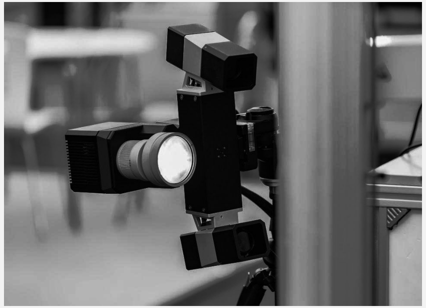
Individual

Group

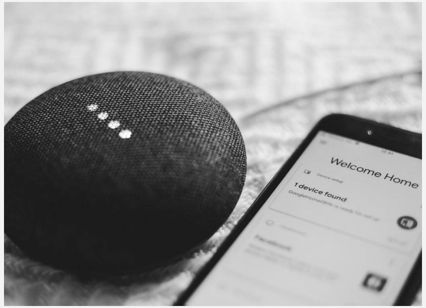
Population

Presence

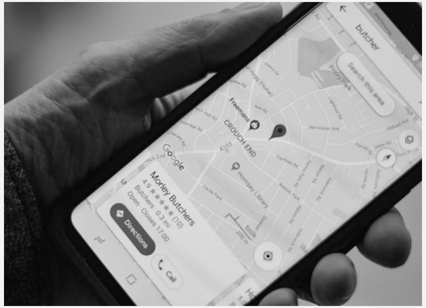
Describes **data which reveals where** an individual, group, or population **has been**.



Motion Sensors



Microphone



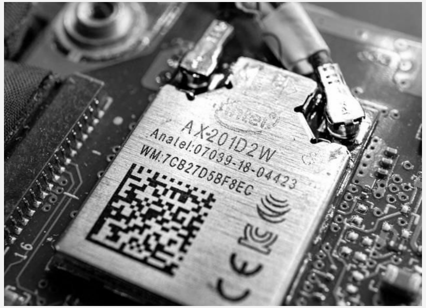
Geolocation

Activity

Describe **data which reveals what actions were performed** by an individual, group, or population.

Activity Monitor

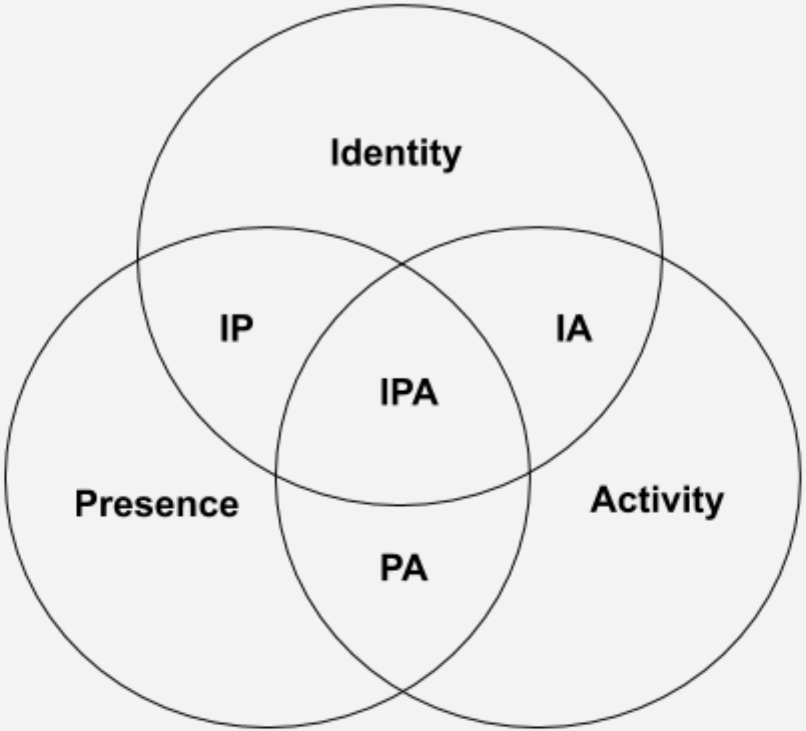
Behavioral Data



Radar Sensor

HMMM...

Venn Time



VIDEO CAMERAS

AUTHENTICATED INTERACTIONS

03

Risk Assessment

A Qualitative Approach

General Methodology

Risk Impact = Severity x Scope x Likelihood

Severity

Scope

Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood

Severity

Scope

Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood

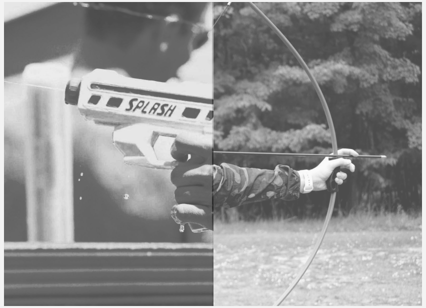
Severity

Scope

Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood



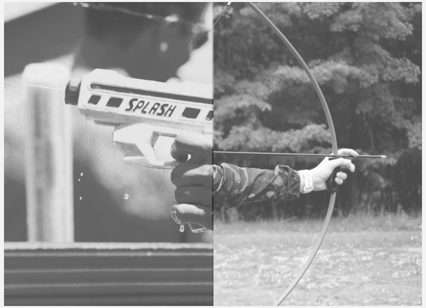
Severity

Scope

Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood



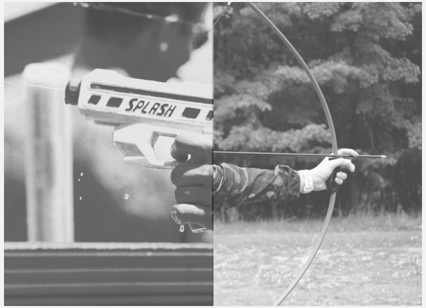
Severity

Scope

Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood



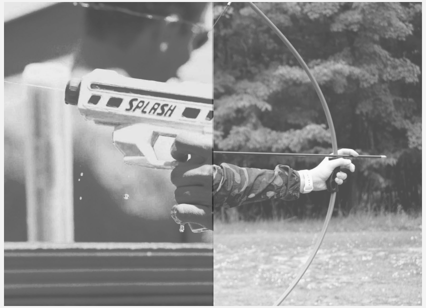
Severity

Scope

Likelihood

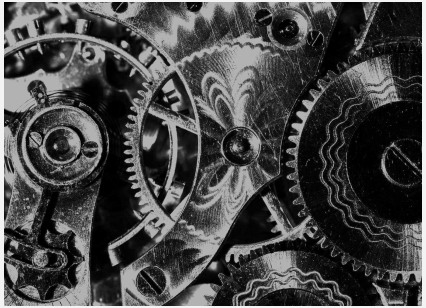
General Methodology

Risk Impact = Severity x Scope x Likelihood



Severity

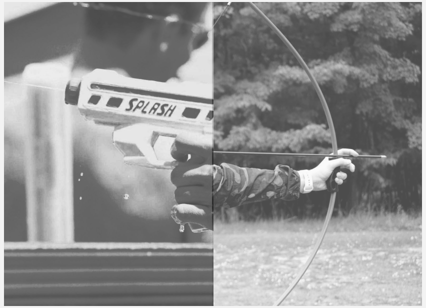
Scope



Likelihood

General Methodology

Risk Impact = Severity x Scope x Likelihood



Severity

Scope

Likelihood

Risk Assessment Matrix

A quick lookup table for calculating risk impact.

Severity				
Low	Medium	High		
Impact			Scope	Likelihood
Low	Low	Low	Low	Low
Low	Medium	Medium	Low	Medium
Low	Medium	Medium	Medium	Low
Medium	Medium	Medium	Medium	Medium
Medium	Medium	Medium	Low	High
Medium	Medium	High	Medium	High
Medium	Medium	High	High	Low
Medium	High	High	High	Medium
High	High	High	High	High

Risk Assessment Matrix

Example: Severity (Low), Scope (Medium), Likelihood (High)

Severity				
Low	Medium	High		
Impact			**Scope**	**Likelihood**
Low	Low	Low	Low	Low
Low	Medium	Medium	Low	Medium
Low	Medium	Medium	Medium	Low
Medium	Medium	Medium	Medium	Medium
Medium	Medium	Medium	Low	High
Medium	Medium	High	**Medium**	**High**
Medium	Medium	High	High	Low
Medium	High	High	High	Medium
High	High	High	High	High

Using IPA Triad Properties

To inform Risk Severity via inferred Data Sensitivity.

	High	Medium	Low
Identity	Very little data is needed to identify individual and would be extremely difficult to forge.	Data may identify individual but repudiation is still possible.	Weak inference of identity, often requires correlating information.
Presence	Strong evidence of human presence (badge scanned)	Possible evidence of human presence (motion detection)	Weak indicator of human presence, may require correlating information.
Activity	Very little data is needed to identify the specific activity taking place.	Data explicitly indicates a general activity but may also imply highly specific activities.	Weak implication of certain activity, may require correlating information.

04

Use Cases

Applying the IPA Triad in Privacy Risk Assessments

Developer APIs

Developer APIs

Android / iOS Permissions

Native authorization framework for app developers to request information from your device.

OAuth 2.0

An authorization framework used mostly everywhere to authorize third-party access to remote services, for better or worse.

Browser Permissions

Native authorization framework for website developers to request information from your browser.

Developer APIs

Android / iOS Permissions

Native authorization framework for app developers to request information from your device.

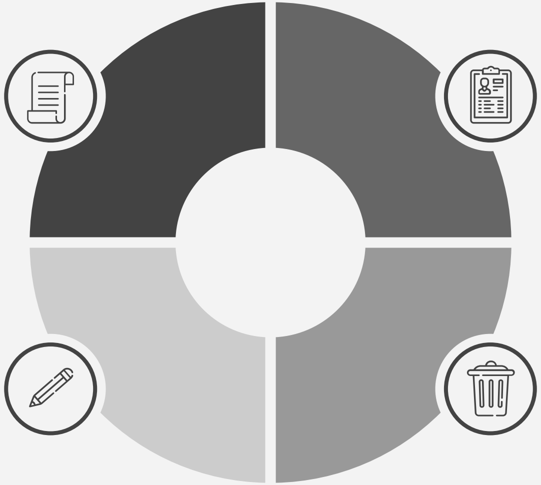
OAuth 2.0

An authorization framework used mostly everywhere to authorize third-party access to remote services, for better or worse.

Browser Permissions

Native authorization framework for website developers to request information from your browser.

Developer APIs Provide Third Party Access to User Data



Create

New records

Read

Existing records

Update

Existing records

Delete

Existing records

Authorization Flow

User Receives Request

Grants Various Permission Scopes

Developer Receives Token; Authorized To Access Any Resource The Scope(s) Allow

Protect Developer APIs

Assess Resources

Use IPA Triad to inform data sensitivity and assess privacy risk for each resource.

Assess Scopes

Aggregate your privacy risk scores for all resources a given permission scope permits access to.

De-Risk Platform

Consider your most sensitive permissions and determine whether you can make scopes more granular.

Protect Developer APIs

Assess Resources

Use IPA Triad to inform data sensitivity and assess privacy risk for each resource.

Assess Scopes

Aggregate your privacy risk scores for all resources a given permission scope permits access to.

De-Risk Platform

Consider your most sensitive permissions and determine whether you can make scopes more granular.

Protect Developer APIs

Assess Resources

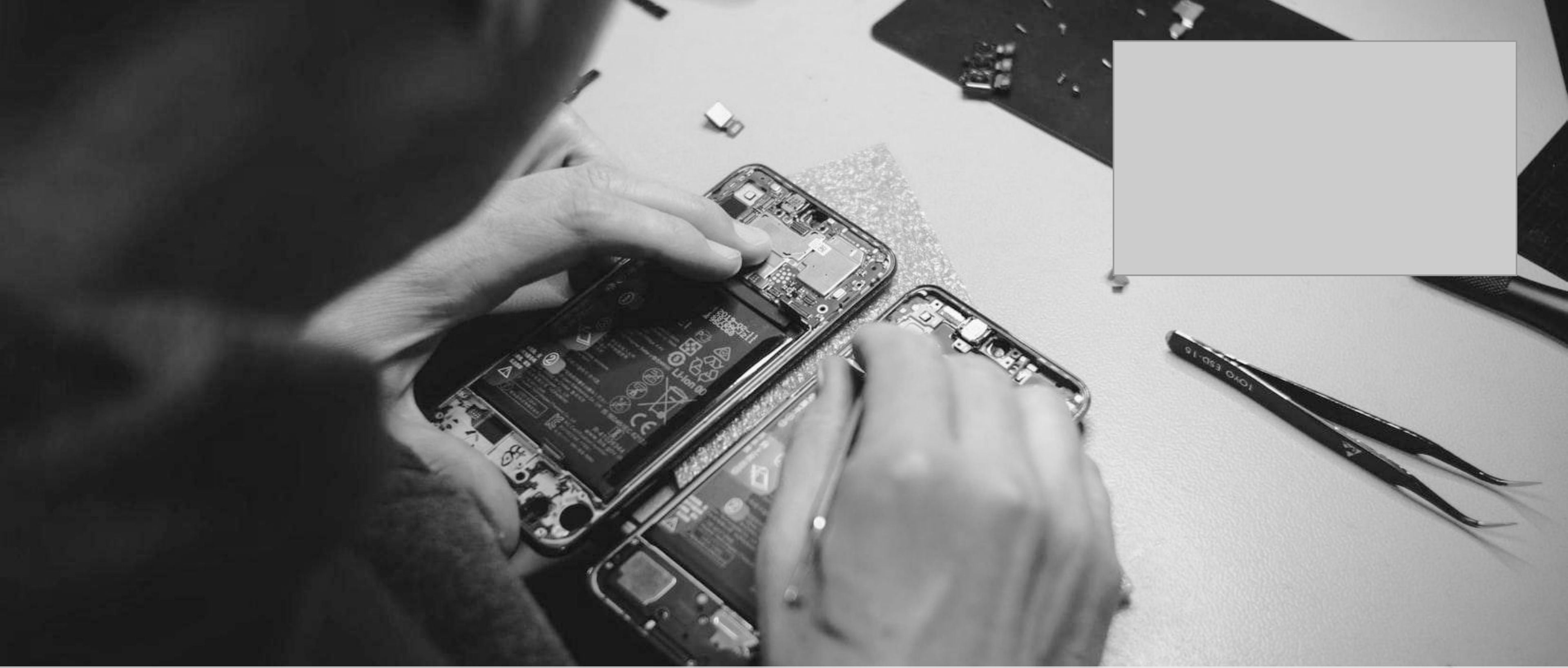
Use IPA Triad to inform data sensitivity and assess privacy risk for each resource.

Assess Scopes

Aggregate your privacy risk scores for all resources a given permission scope permits access to.

De-Risk Platform

Consider your most sensitive permissions and determine whether you can make scopes more granular.



Device Sensors

Let’s borrow another security concept

Let’s borrow another security concept

Side-channel attacks:

(para) Using information to make inferences based on underlying device / software implementation.

https://en.wikipedia.org/wiki/Side-channel_attack

Device Sensors

What kinds of side-channels might they be into a target’s identity, presence, or activity?

Heart Rate

GPS

Air Quality

Device Sensors

What kinds of side-channels might they be into a target’s identity, presence, or activity?

Heart Rate

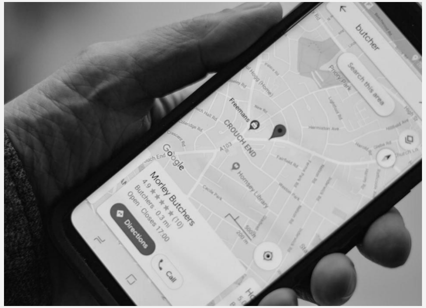
GPS

Air Quality

Device Sensors

What kinds of side-channels might they be into a target's identity, presence, or activity?

Heart Rate



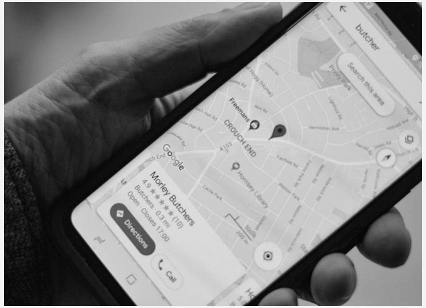
GPS

Air Quality

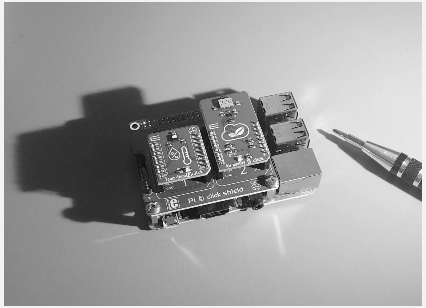
Device Sensors

What kinds of side-channels might they be into a target’s identity, presence, or activity?

Heart Rate



GPS



Air Quality

Protect Sensor Data

Review Capabilities

What is the device capable of inferring about identity, presence, or activity?

Isolate Processing

What actually needs to be exposed for external processing?

Degrade Signal

For data that must be externally processed, can you reduce the fidelity of data exposed?

Protect Sensor Data

Review Capabilities

What is the device capable of inferring about identity, presence, or activity?

Isolate Processing

What actually needs to be exposed for external processing?

Degrade Signal

For data that must be externally processed, can you reduce the fidelity of data exposed?

Protect Sensor Data

Review Capabilities

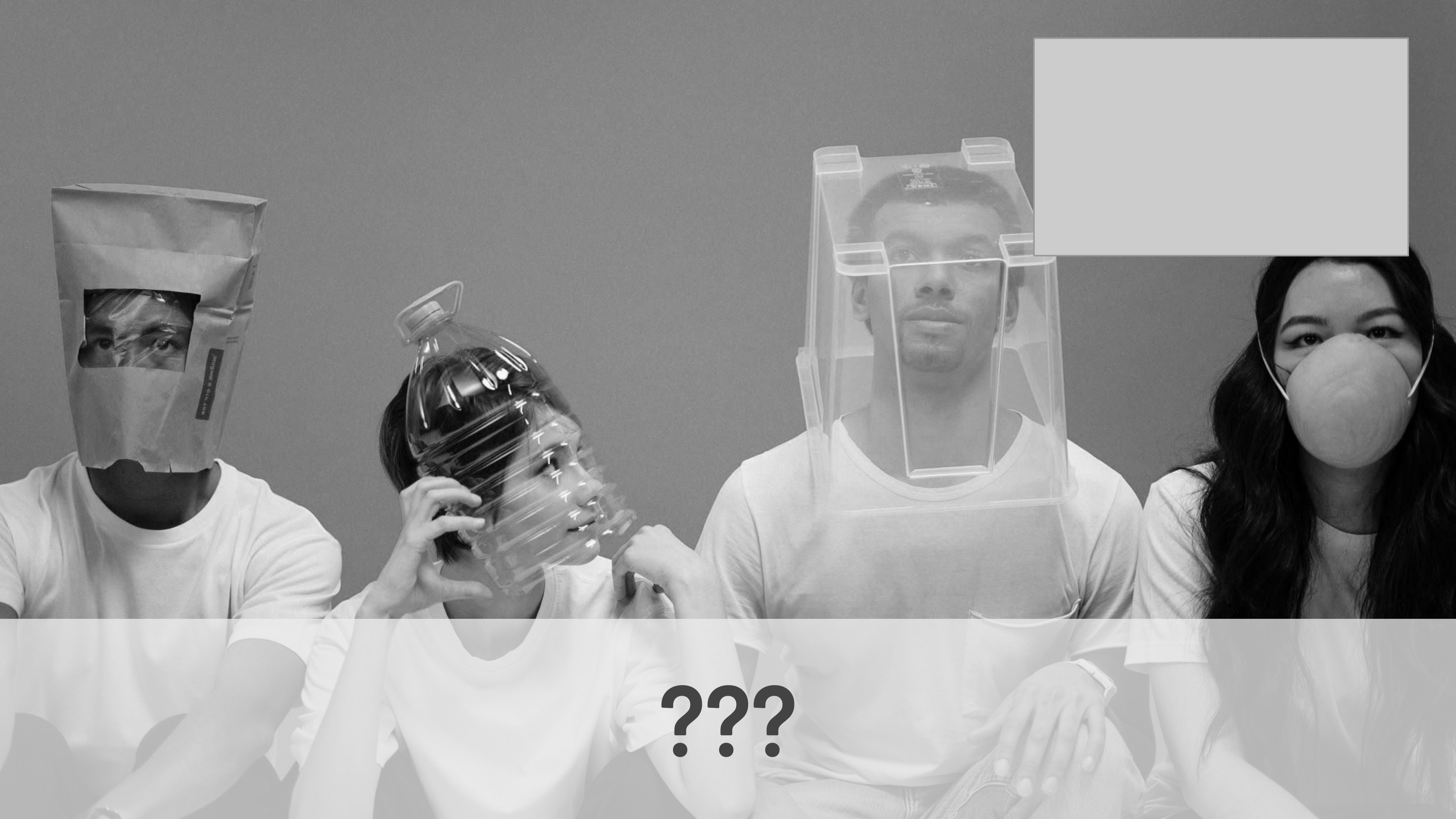
What is the device capable of inferring about identity, presence, or activity?

Isolate Processing

What actually needs to be exposed for external processing?

Degrade Signal

For data that must be externally processed, can you reduce the fidelity of data exposed?



???

THANKS!

Do you have any questions?

pepr2020@obscure.group

CREDITS: This presentation template was created by **Slidesgo**,
including icons by **Flaticon**, and infographics & images by **Freepik**