



Privacy Principles for PAT

DISCLAIMER: I AM NOT THE TAG



FLAMMABLE



CHEMICAL WEAPON



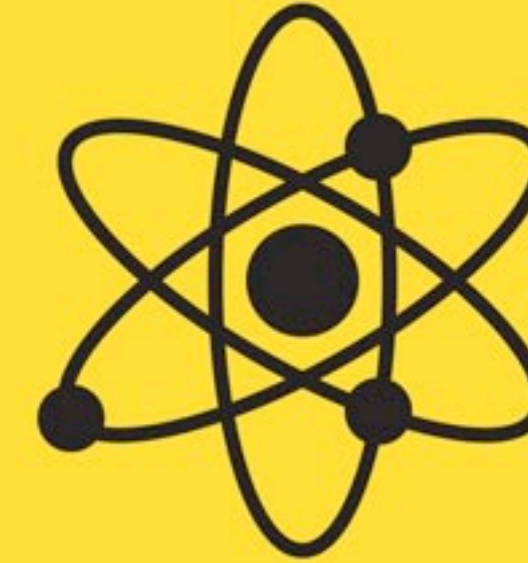
TOXIC



RADIOACTIVE



BIOHAZARD



ATOMIC



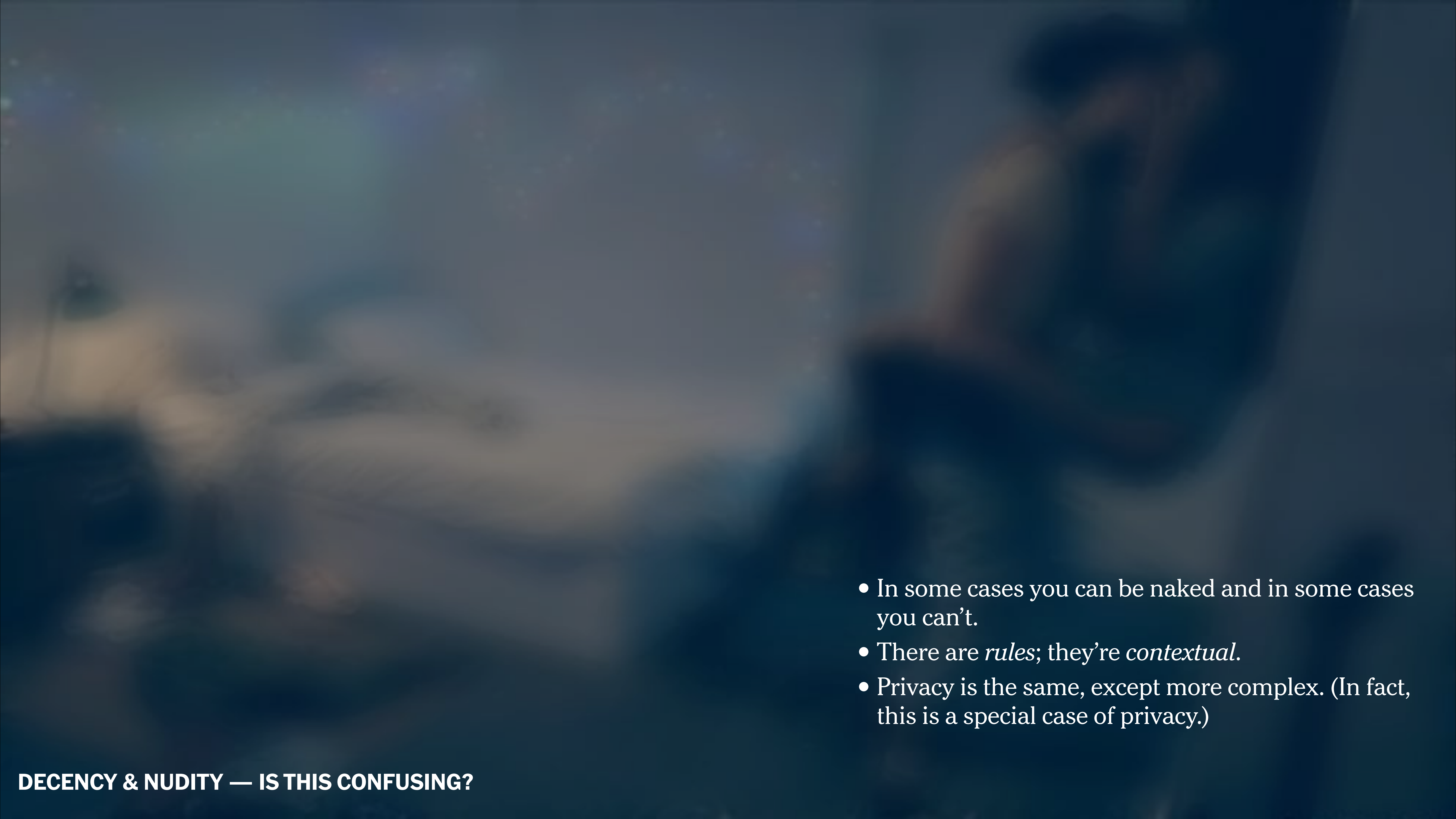
CAUTION



LASER RADIATION



HIGH VOLTAGE

- 
- In some cases you can be naked and in some cases you can't.
 - There are *rules*; they're *contextual*.
 - Privacy is the same, except more complex. (In fact, this is a special case of privacy.)



DATA GOVERNANCE

Data governance regulates information flows.

Privacy is a subset of data governance

It governs flows that are either about people or that impact them.

Governance works with rule systems

The rules describe how given actors, in given contexts, may/must/must not process information from, to, or about others.

REAL-WORLD GOVERNANCE

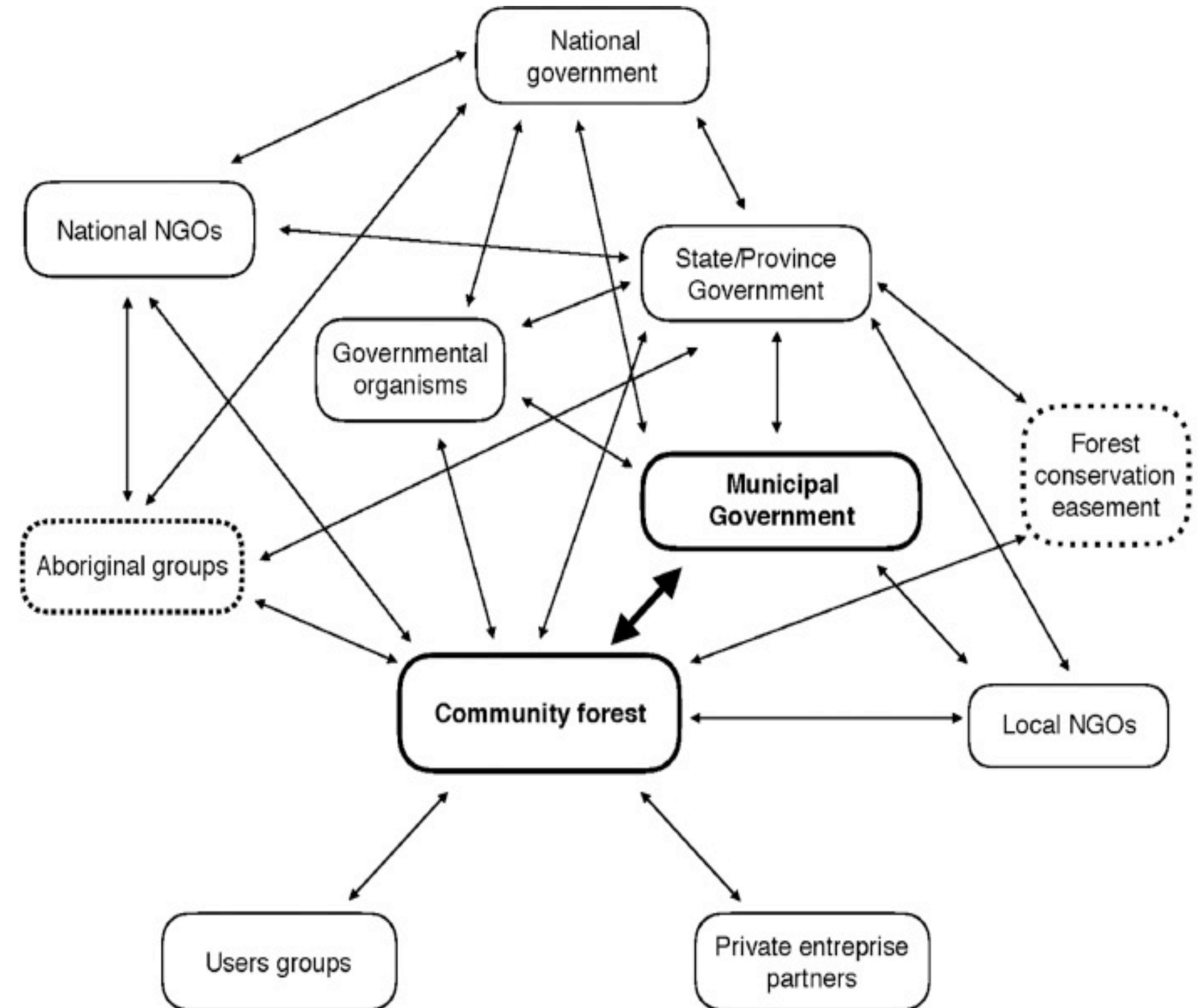
Real-world governance systems are intricate and complex.

Contexts nest, overlap, intermesh

For any given situation, multiple rule systems will apply at once. (And that's okay! It's robust.)

We have our context

The TAG can look at the Web in broad terms; PAT can take more specific. We can be more restrictive (eg. on consent) and we can open narrow exceptions (eg. learning a sliver of information for attribution).





IT CAN TAKE TIME FOR RULES TO EMERGE

Privacy Principles

W3C Draft TAG Finding 25 March 2022



▼ More details about this document

Latest editor's draft:

<https://w3ctag.github.io/privacy-principles/>

History:

[Commit history](#)

Editors:

[Robin Berjon \(The New York Times\)](#)

[Jeffrey Yasskin \(Google\)](#)

Feedback:

[GitHub w3ctag/privacy-principles \(pull requests, new issue, open issues\)](#)

Copyright © 2022 W3C® (MIT, ERCIM, Keio, Beihang). W3C [liability](#), [trademark](#) and [permissive document license](#) rules apply.

Abstract

Privacy is an essential part of the Web ([[ETHICAL-WEB](#)]). This document provides definitions for privacy and related concepts that are applicable worldwide. It also provides a set of privacy principles that should guide the development of the Web as a trustworthy platform. People using the Web would benefit from a stronger relationship between technology and policy, and this document is written to work with both.

<https://w3ctag.github.io/privacy-principles/>

A few high-level considerations

DRAWN FROM THE TAG PRINCIPLES



AVOID ASYMMETRIES OF POWER

Information is power. Concentrations of information are concentrations of power.

We protect people from asymmetries of power
By helping avoid the excessive concentration of information in one single place, we protect people — notably against nudging.

RESPECT INDIVIDUAL AUTONOMY

All people deserve the right to exercise their autonomy without undue interference and with full respect for their values, preferences, and beliefs.

Notice & choice

Respecting people requires us to account for bounded rationality and deceptive patterns. Digital advertising processing is not consentable.

Privacy labo(u)r

To the extent possible we seek to avoid offloading to people the work to ensure that their privacy is respected.



PRIVACY CALLS FOR COLLECTIVE GOVERNANCE

Modern privacy issues are inferential and statistical. Because of this, the data of one person can reveal information about many others.

We need a collective approach

Individualistic solutions cannot adequately address the risks that stem from inferences drawn from someone else's data.

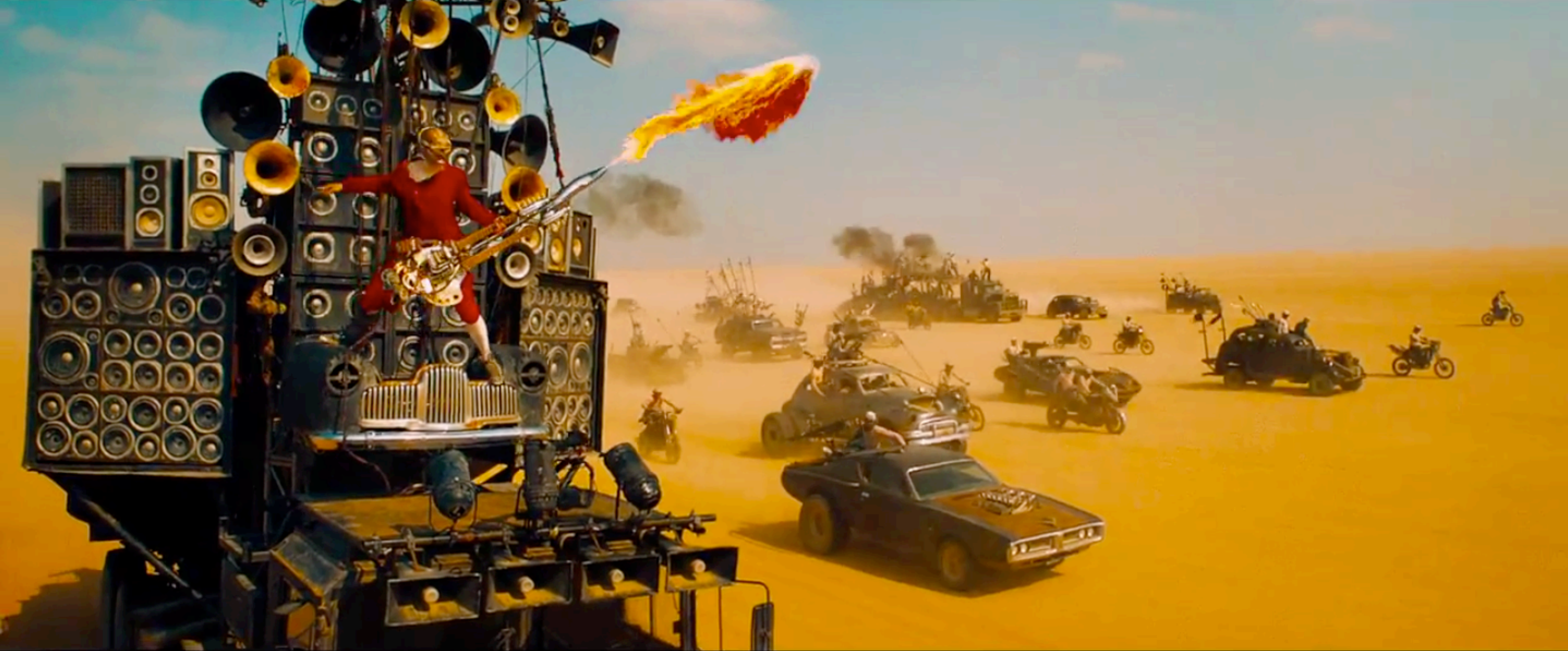
The approach needs to be context-specific

Collective decisions need to be made in ways that are relevant to specific contexts. For various parts of the Web, this makes Internet governance & standards a logical avenue.

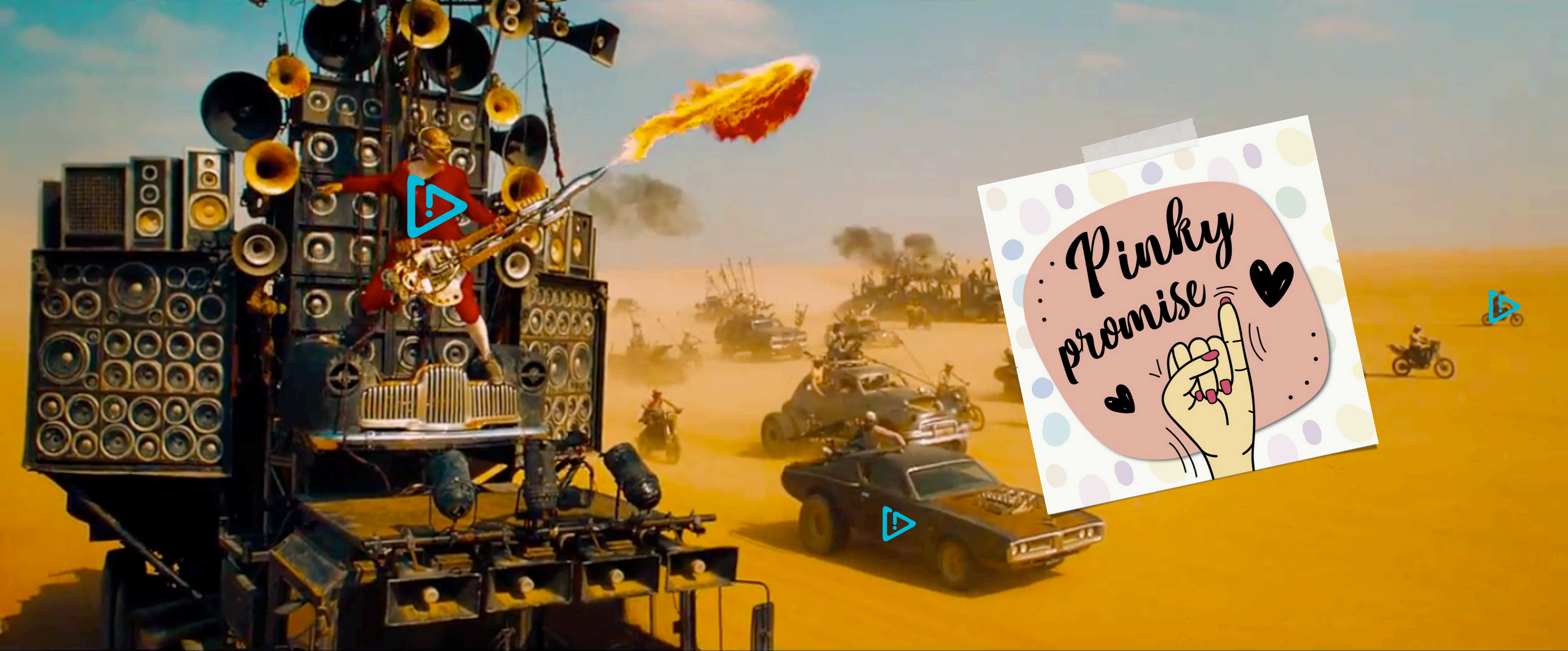


Where do we go
from here?

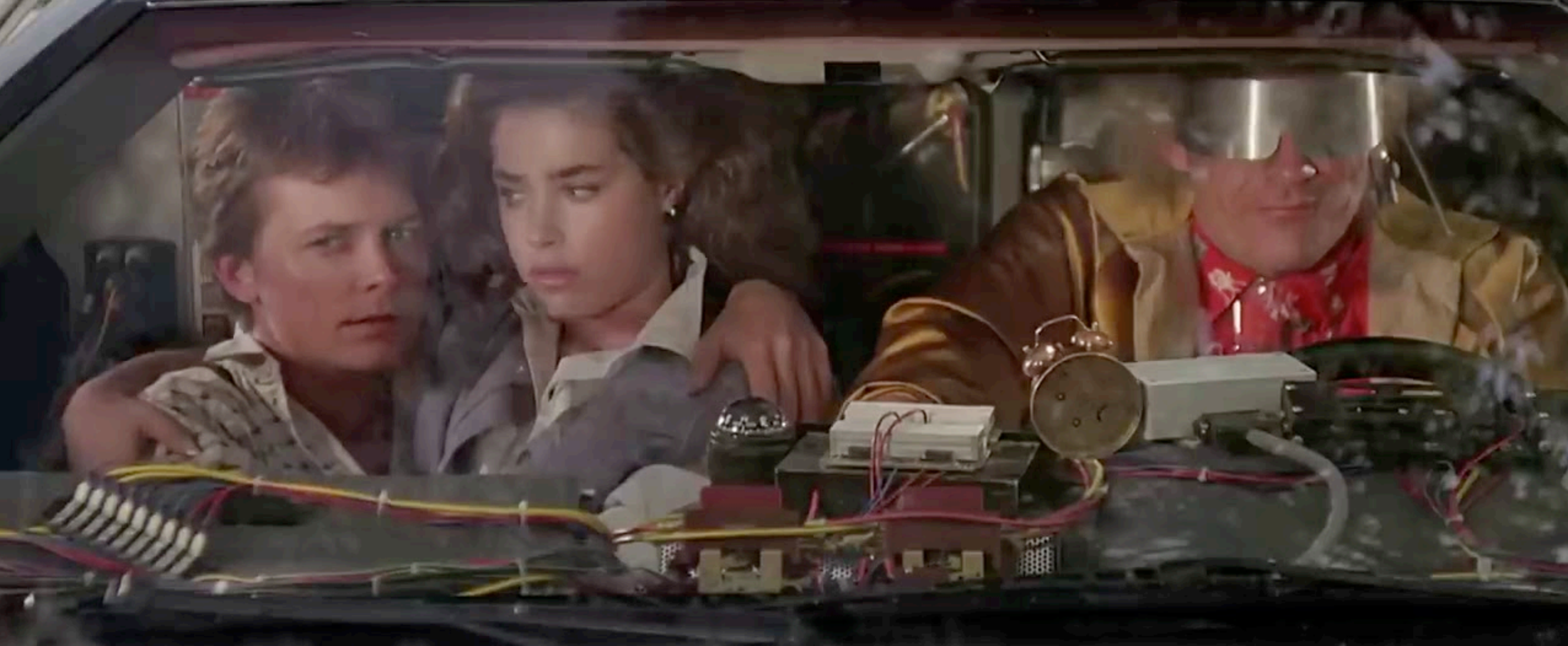
THERE ARE SEVERAL POSSIBLE RULE SETS



ALL DATA **MUST** BE MADE AVAILABLE TO ANY PARTY PRESENT.



ALL DATA **MUST** BE MADE AVAILABLE TO ANY PARTY PRESENT.
PEOPLE **MAY** OPT OUT BY GOING TO A SEPARATE SITE AND NEVER CLEARING THEIR COOKIES.
COMPANIES **MUST** HAVE CONTRACTS WITH ONE ANOTHER IN WHICH THEY PROMISE TO THINK GOOD THOUGHTS.

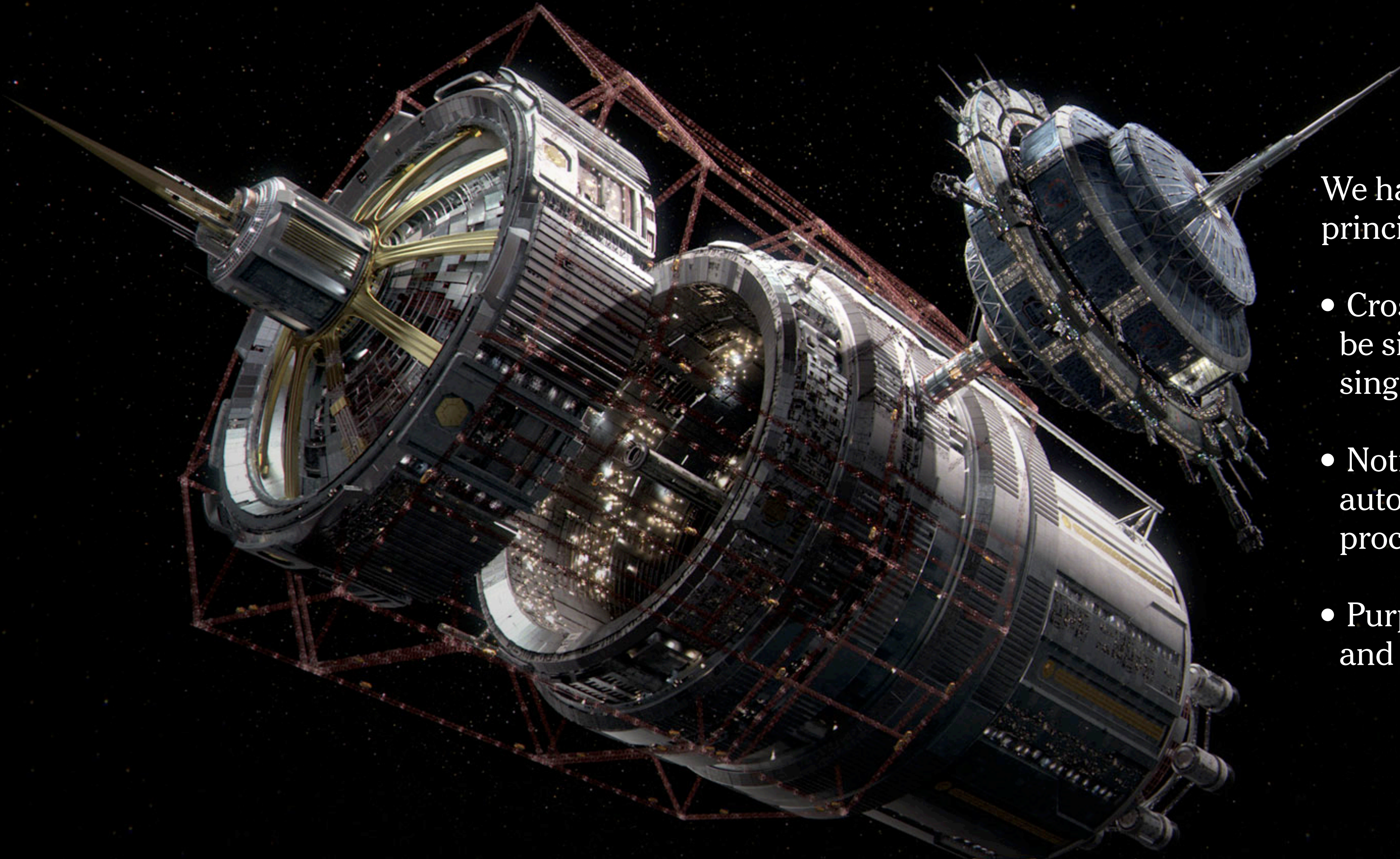


ADS **MUST NOT** BE TARGETED TO INDIVIDUALS.
ADS **MUST NOT** MAKE USE OF PERSONAL DATA AS PART OF THEIR LIFECYCLE.

We don't "*define privacy*" but we ground our decisions in principles and we document where those principles lead.

We have candidate PAT-specific principles we can already work on:

- Cross-context reading history *must not* be significantly concentrated with a single entity.
- Notice & choice *must not* to support autonomy with respect to advertising processing.
- Purpose limitations *must* be enforced and guaranteed to the extent possible.



Thank you!

Robin Berjon • robin@berjon.com • [@robinberjon](https://twitter.com/robinberjon)

