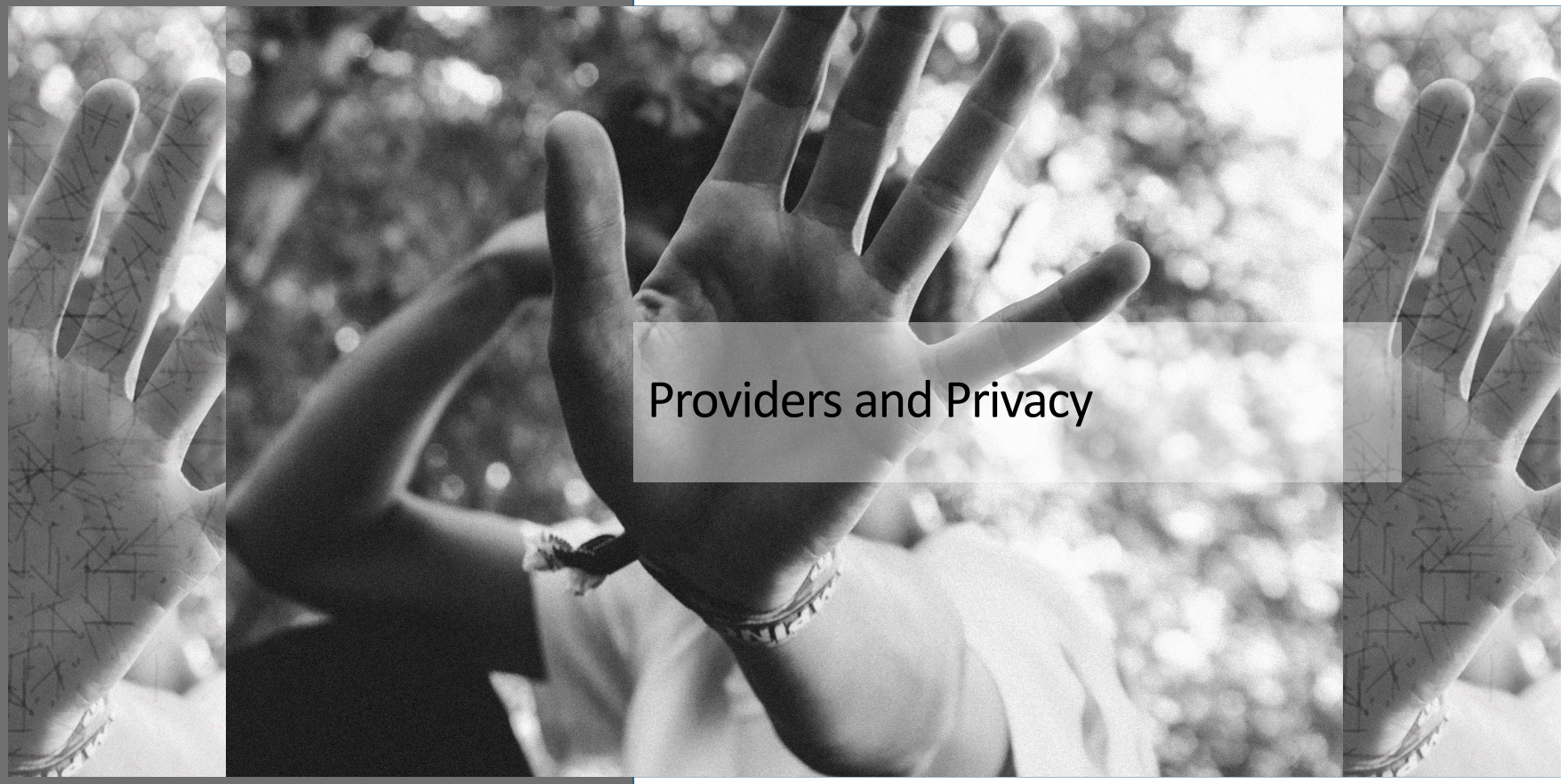


Providers and Privacy

Russ White

russ@riw.us

If you have done nothing wrong, you have nothing to hide...

The plea for privacy is often a plea for the right to misrepresent one's self to the rest of the world.

Richard A. Epstein, "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology," Boston University Law Review 74.1 (1994): 12

GDPR

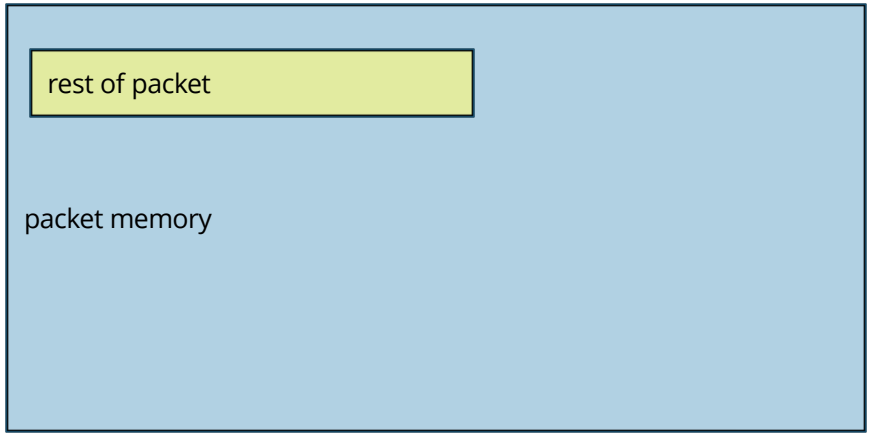
… any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

HIPAA

… data can be considered nonidentifiable after the removal or generalization of 18 specific types of potentially identifying information

Birth dates no finer grained than a year, postal code must encompass at least 20,000 people, etc.

do packets contain sensitive information?



is processing packets disclosure?

Property	Explanation
Identifiability	Degree to which the data identifies an individual user
Network centricity	Extent to which information remains local to the client
Confidentiality	Extent to which information is accessible by others
Availability	Extent to which data is available when required by an authorized entity
Integrity	Extent to which the system maintains reliable state without error
Mobility	Extent to which the system moves between locations or devices

Use	Explanation
Primary	The reason the data was collected in the first place; what the user expects
Secondary	Data use outside the original scope; what the user does not expect

Property	In network forwarding devices
Identifiability	Questionable
Network centricity	Definition dependent
Confidentiality	High
Availability	Variable
Integrity	High
Mobility	Doesn't seem to apply

Use	Explanation
Primary	Yes
Secondary	No

Bottom Line

Privacy when *processing* packets is probably not a big deal *because…*

- The privacy value of the information being used is questionable
- It’s being used for it’s primary purpose
- The confidentiality of the information is relatively high

Bottom Line

What about data *inside* the packet?

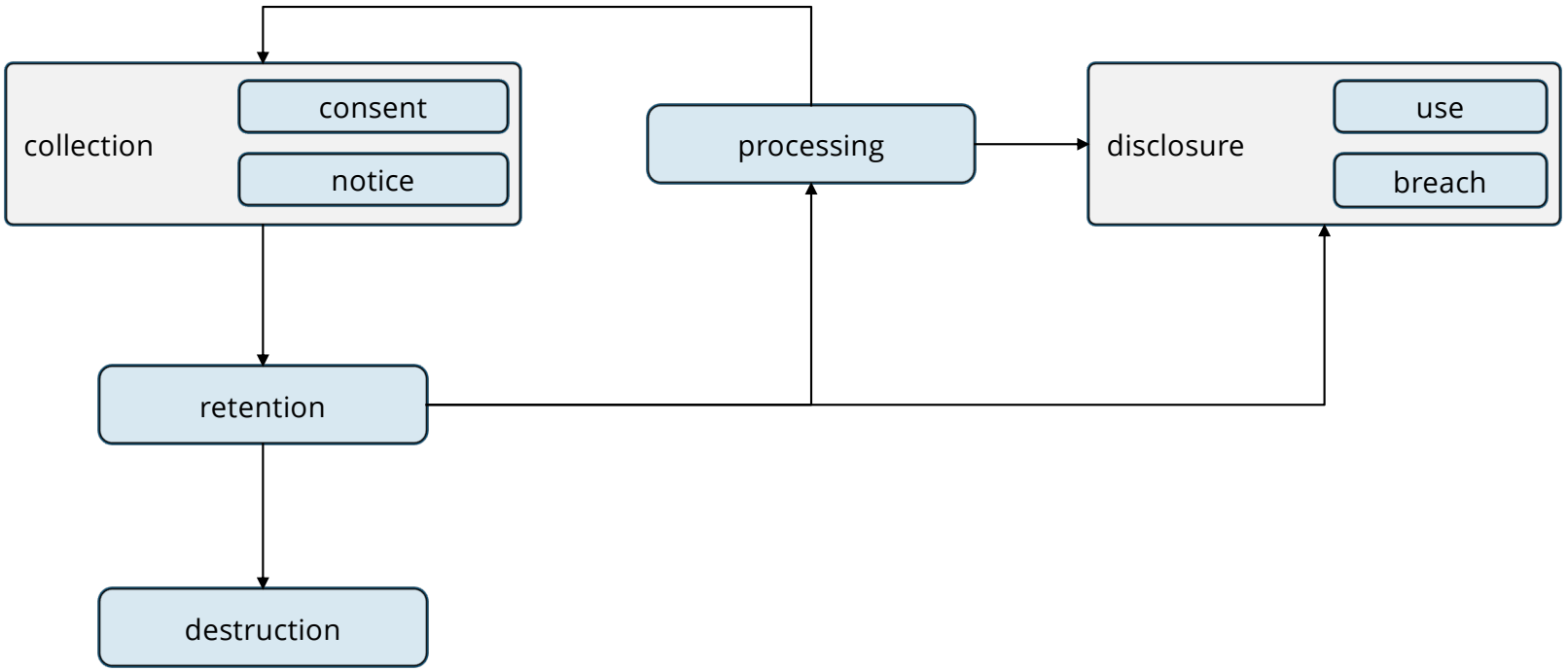
- Other than end-to-end encryption, there's little transport services can do about this
- Largely unexplored space

Logging is where things get a lot more interesting …

- IP address
- Where users are
- When users are active
- What users are accessing
- DNS queries and responses
- Access credentials

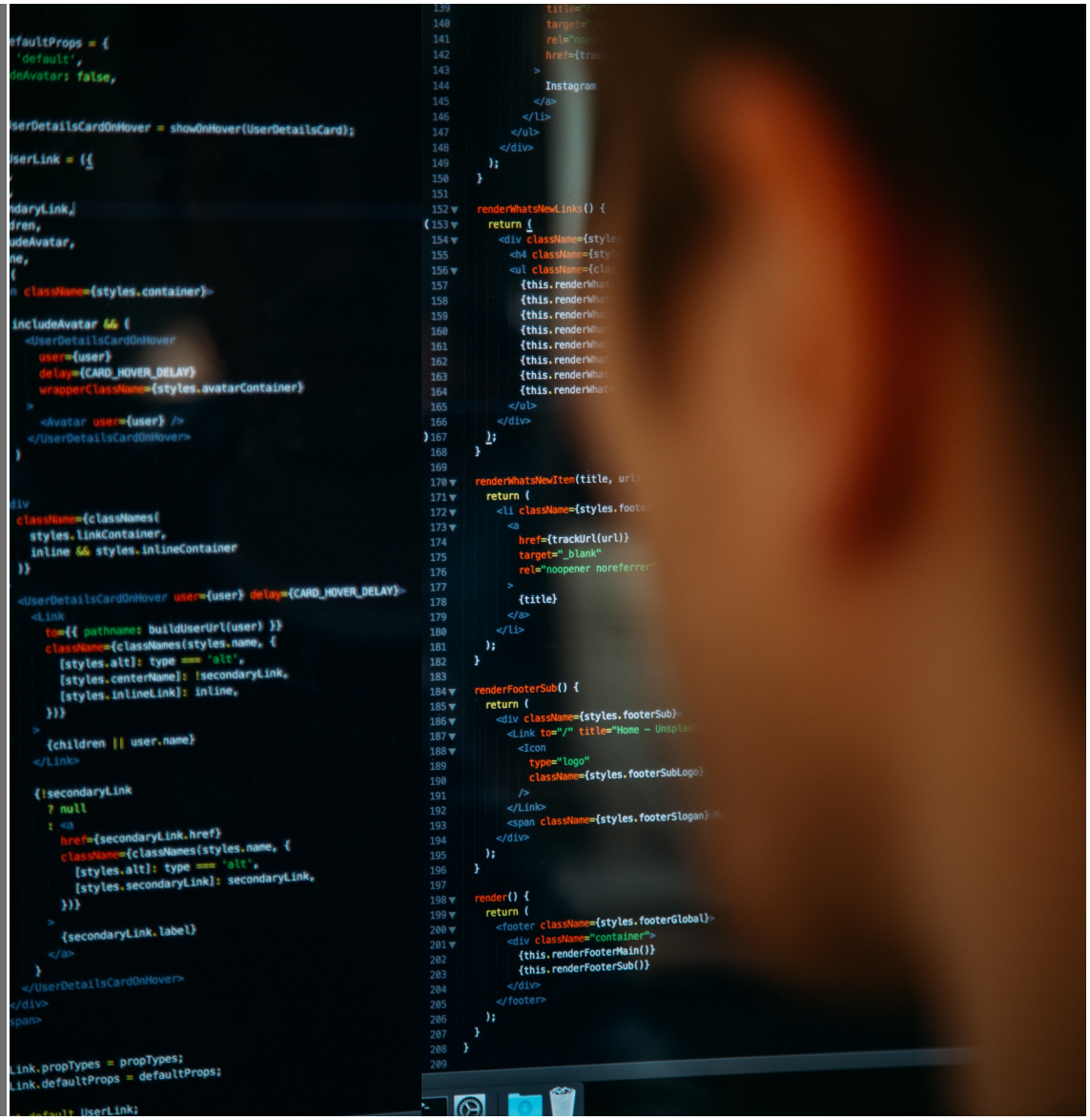
logging

data lifecycle

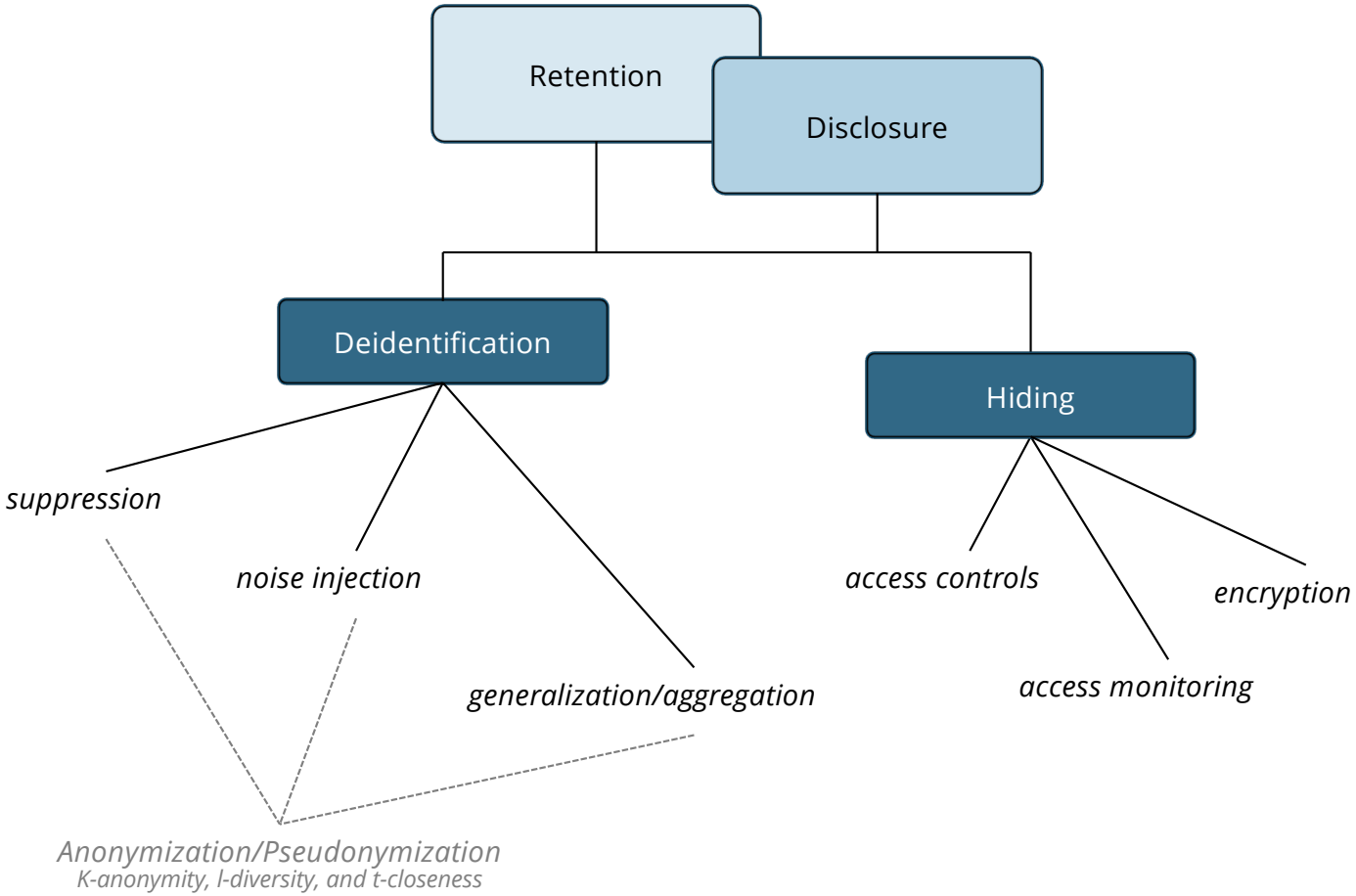


Consent and notice should be part of your contract with all customers

Collection, retention, use, and destruction policies



privacy practices



retention and use

User Right	Notes	Applicable
Access	Users have the right to access the data the provider has about them	Strongly possible
Reification	Users have the right to correct information the provider is storing about them	No
Deletion	Users have the right to ask you to delete any data the provider has about them	Probably (for some kinds of information)
Restriction	Users have the right to restrict who the provider shares information about them with	Strongly possible
Portability	Users have the right to take their data to another provider	No
Against automated decision making	Users have the right to use the service without their data being used to determine advertising displayed or offered choices	Probably
Private action	Users have the right to take legal action against the provider (beyond any action regulatory agencies might take)	Yes

- *These are the common sorts of rights privacy legislation gives users*
- *To my knowledge, no-one has applied these to any transit provider*
  - *Just organizations like content providers, retailers, etc.*
  - *This doesn't mean they don't apply, just I can't find specific information*

You need to take privacy seriously

Legal landscape is changing constantly

Move towards a position of mitigating risk rather than focusing on legal compliance

bottom line

Thank you!

If you have questions, please feel to get in touch