Trust and ethical frameworks for IoT

ICTP Trieste,
July 2017

Robin Wilton
Technical Outreach Director, Trust and Identity
wilton@isoc.org

ISOC is 25 this year!

Password disclosure at borders

…

Encryption backdoors

…

Content blocking

…

Internet Society speaks out against proposed password disclosure requirements

21 February 2017 Public Policy

Today, the Internet Society, along with 50 organizations and trade associations and nearly 90 individual experts who care deeply about an open, trusted Internet, expressed our deep concerns that the U.S. Department of Homeland Security may require individuals to disclose their social media account passwords as a condition of entry into the United States. Last week, the new U.S. Secretary of Homeland Security indicated that the U.S. government is considering such a policy as an element of border screening.

We signed onto this statement because we believe that this policy would gravely undermine Internet security and would represent an alarming intrusion on individuals' rights of expression, opinion and privacy. We also worry that other nations may replicate this approach, leading to a cascading decline in Internet security for users across the globe.

Global Presence

110+	72k	146	5	18
Chapters Worldwide	Members and Supporters	Organization Members	Regional Bureaus	Countries with ISOC Offices

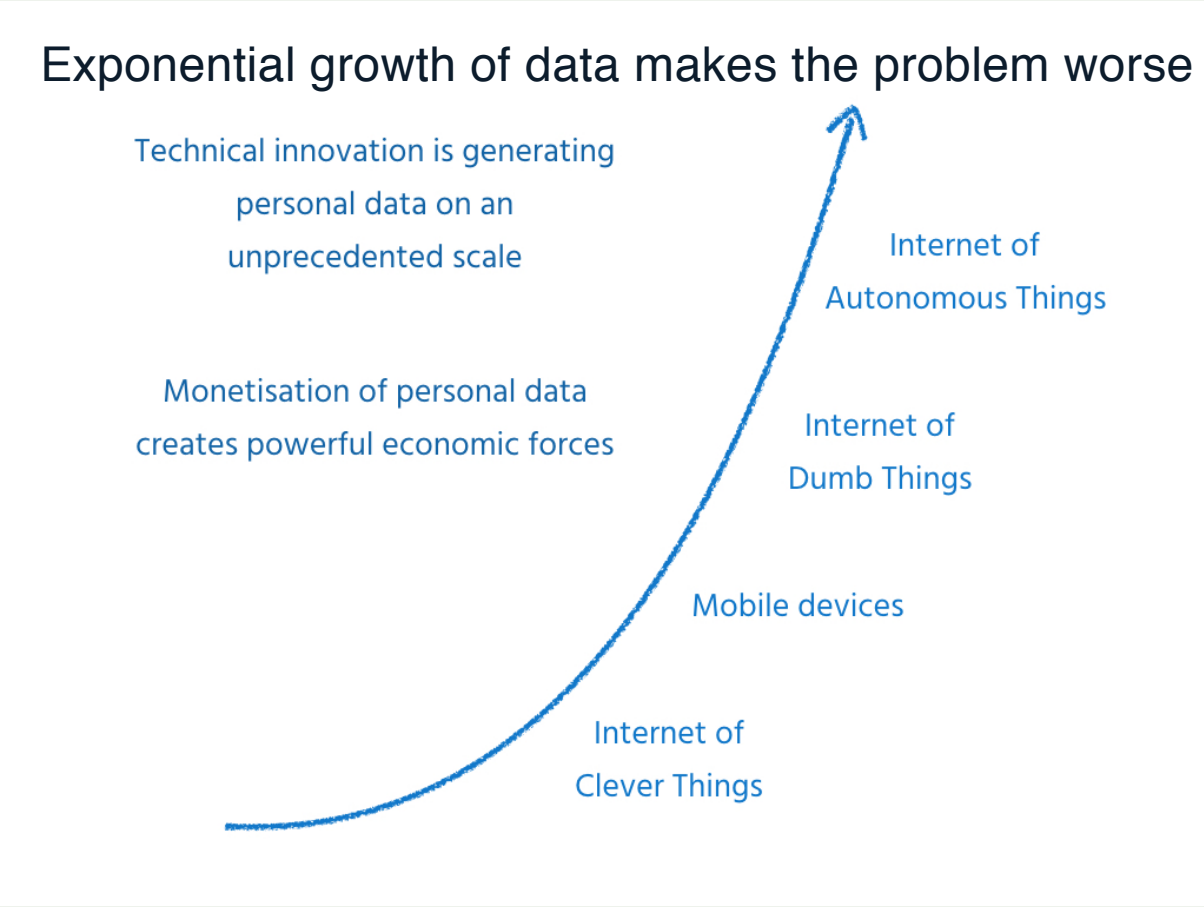
Data protection/compliance is falling short of protecting consumers

The data protection approach to protecting privacy is over 35 years old

In the consumer space, outcomes are still poor:

- Apps and objects that gather data not associated with their function
- A data monetisation ecosystem that compromises users' privacy
- "Consent" notices that flout the spirit of the law (for instance, on cookies)

Poor outcomes damage user trust and adoption



Increased centralisation of data

Machine-to-machine connectivity intensifies data collection and aggregation

The bulk of this data will be about users

Such a surge in the volume of centralised data is bound to have a profound impact on individual privacy

Some implications of the IoT phenomenon

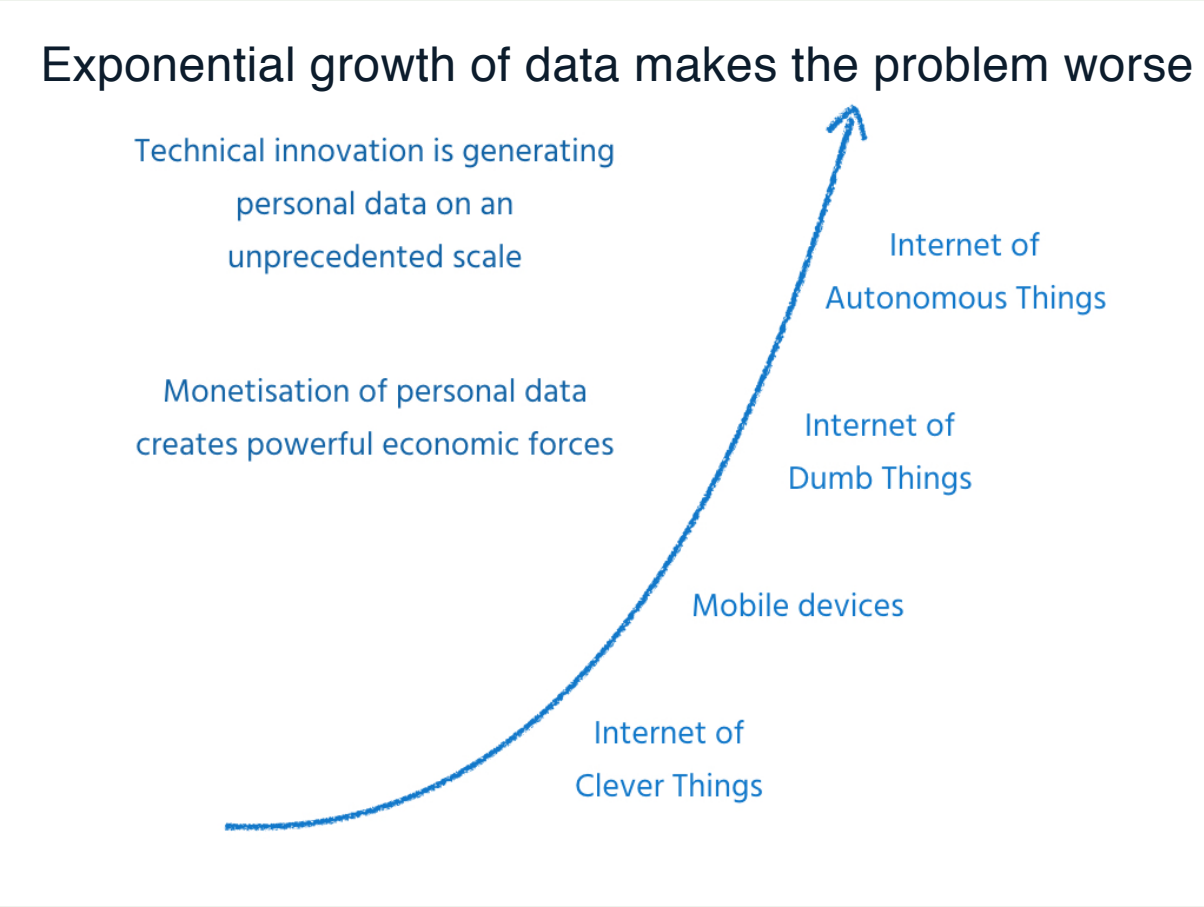
Data growth is (approximately) exponential:

Human capacity is (approximately) constant.

- Increasingly, such data will only be comprehensible to humans if filtered/ modelled

Devices become, instead of objects used by humans, intermediaries between humans and an ecosystem of third parties.

- The user interface only tells part of the story



A Recent, Real-World Example

- Share your child's intimate thoughts with random strangers!
- Pay for the toy,
- Pay again with your data,
- Pay again when the data is ransomed!
- No need to worry about security, simply enable Bluetooth on your phone!

- One retail product, aimed at young children
- Over 800,000 accounts/profile photos compromised
- Over 2 million voice recordings exposed

Increased third party mediation

IoT gives rise to models and approaches that undermine human agency

The devices that we use for specific tasks may be doing other things without our knowledge or consent, but which will affect us directly or indirectly

With IoT, much of our offline activities will be digitally mediated as well

Lessons from the connected toy

- Security of the device was not designed in
- Security of the back end was not designed in
- What value set does this approach indicate?

- Securing IoT devices increases their cost
- But there’s a cost to insecurity, too
- Especially for objects with a longer life-span

- Values-based design is a viable option: plenty of guidance is available

The Internet Society Calls for an Ethical Approach

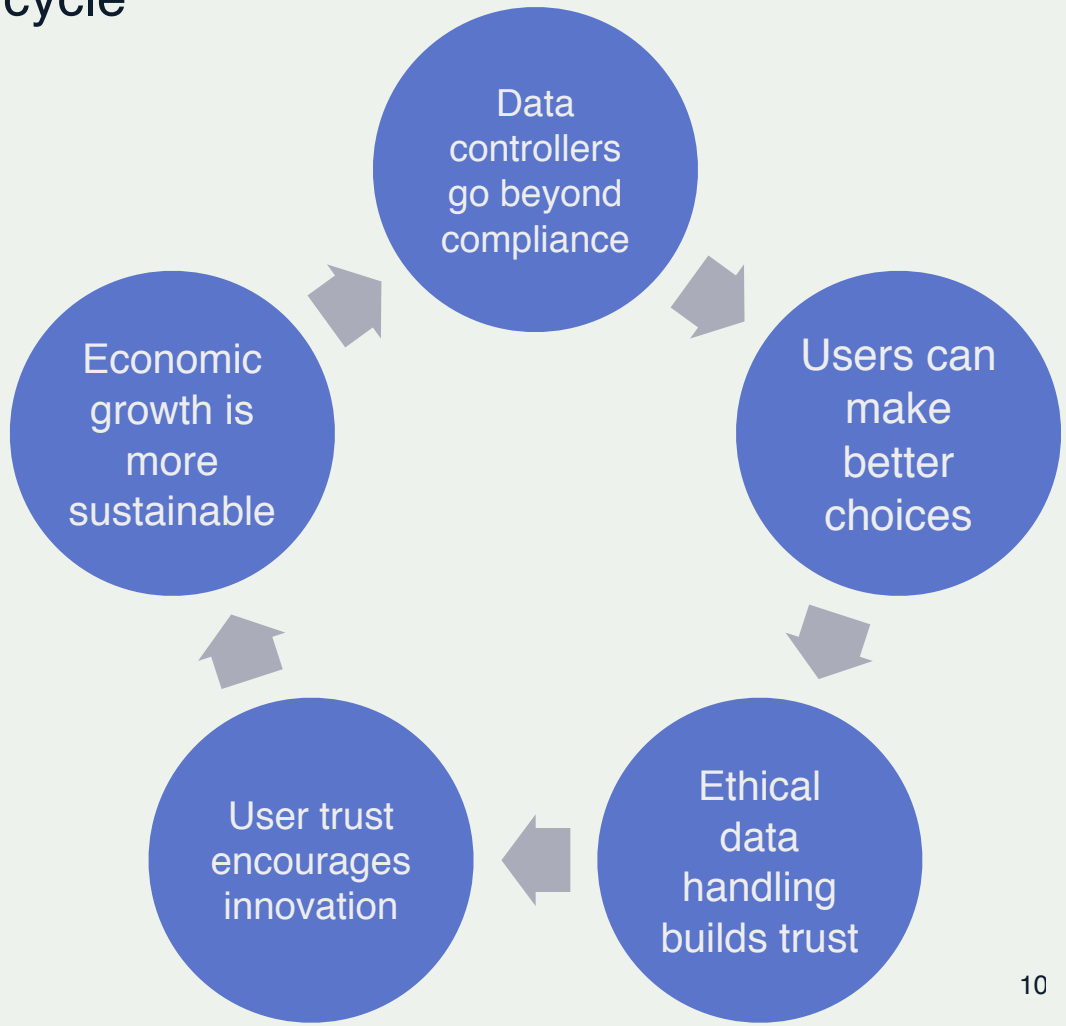
For users:

- Clear guidance at the point of decision
- Transparency of data usage
- Effective accountability and redress

For data controllers:

- Practical guidance about ethical design
- A clear trust framework for certification
- Cross-border audit and accountability

Ethical data handling creates a virtuous cycle



Making Ethical Data Handling The New Norm

Consumers/citizens:

- Consider the values that your choices reflect
- Cultivate those habits that protect your interests
- If necessary, “vote with your feet” (or your wallets)
- Press for – and use - appropriate tools

In a data-driven economy, we are all stakeholders – and we should all act accordingly

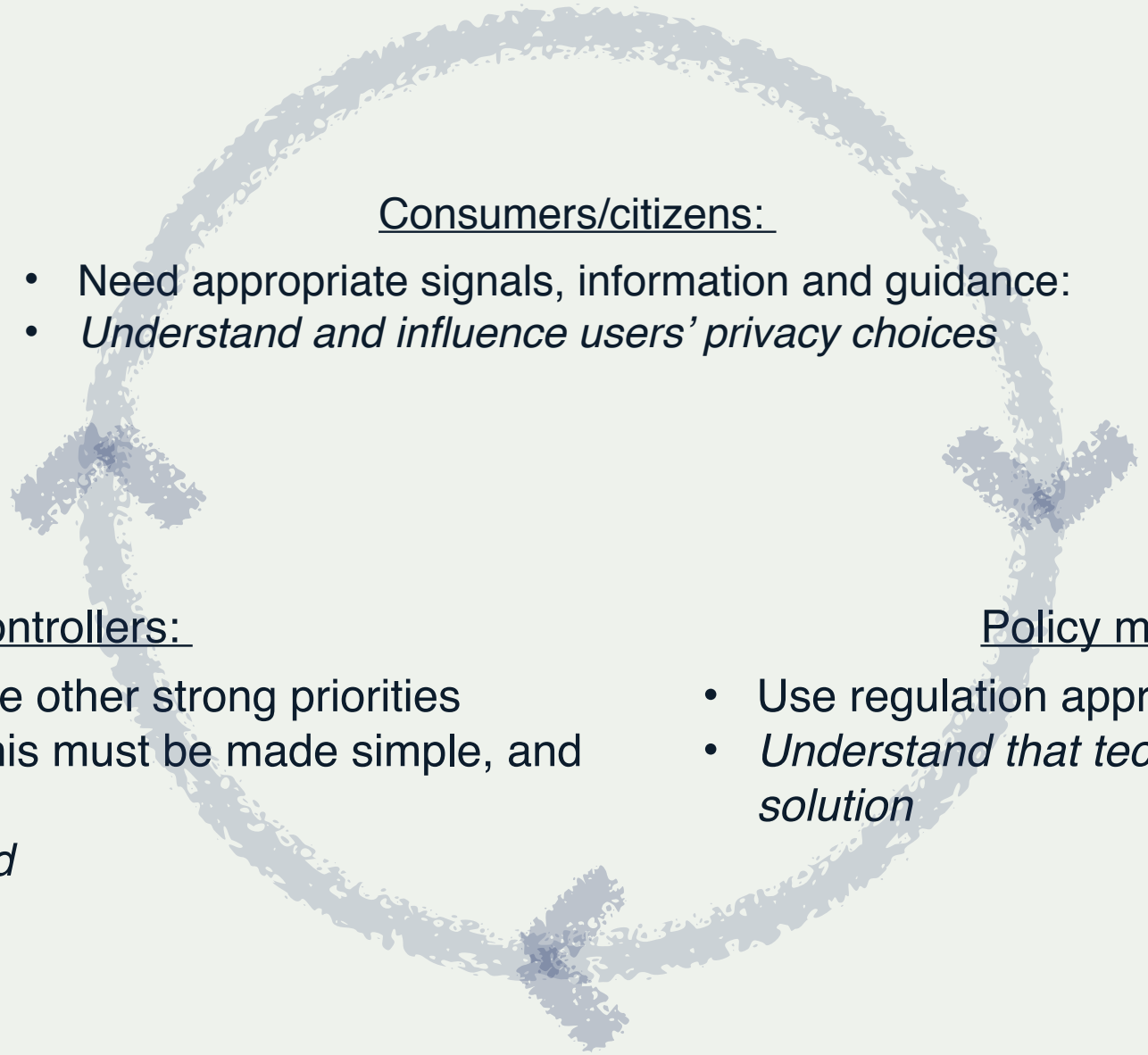
Data controllers:

- Publish ethical data commitments and stand by them
- Be honest and fair about consent and re-use
- Be transparent about your business model
- Embody ethics in product/service design

Policy makers:

- Pre-empt or correct market failures
- Prioritise *sustainability* in the data-driven economy
- Use the available measures:
  - Education, awareness-raising
  - Economics
  - Regulation

Point solutions don’t address systemic issues



Consumers/citizens:

- Need appropriate signals, information and guidance:
- *Understand and influence users’ privacy choices*

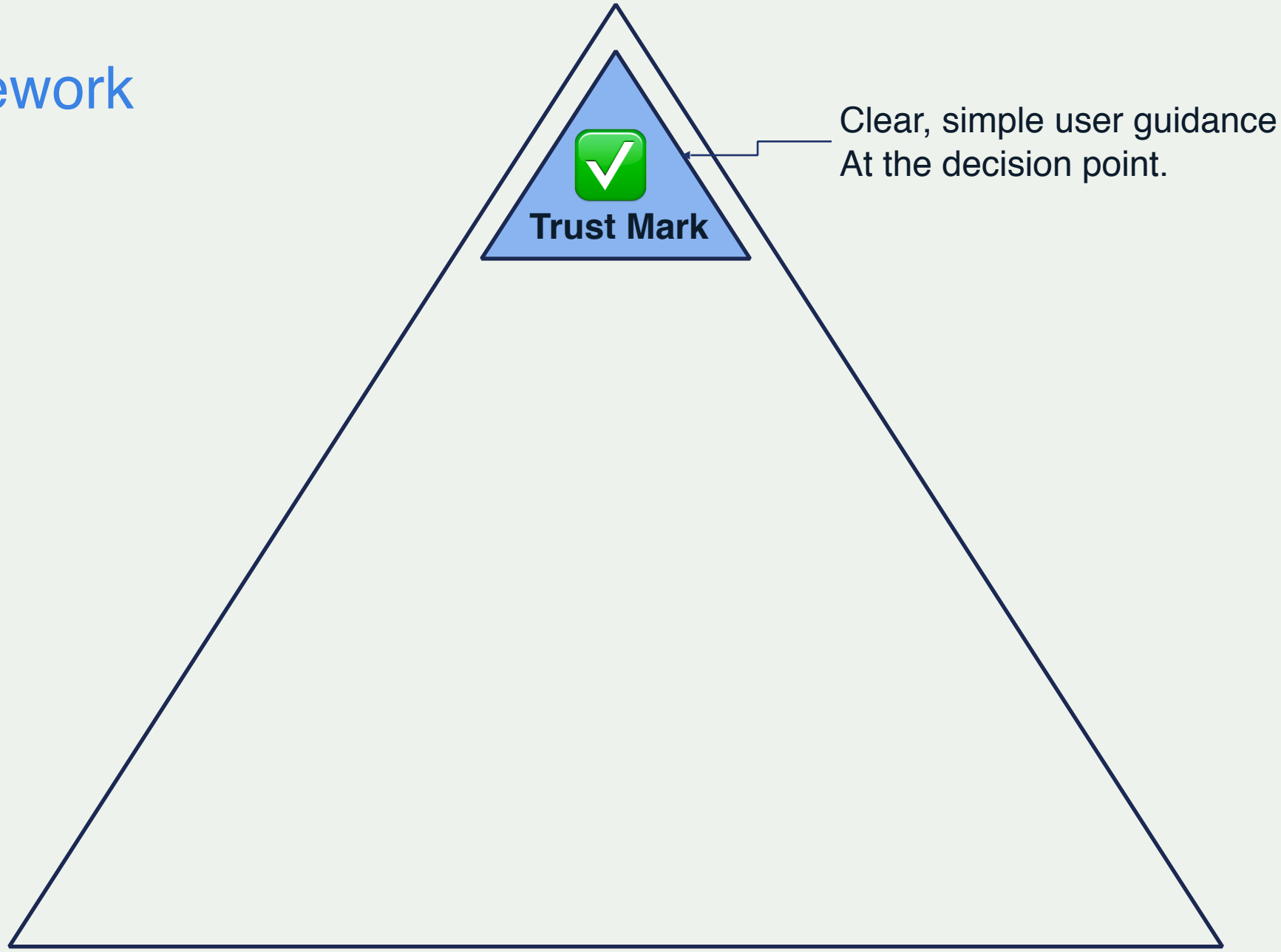
Data controllers:

- Most data controllers have other strong priorities
- Data controllers’ part in this must be made simple, and aligned with their goals
- *Look for the trust dividend*

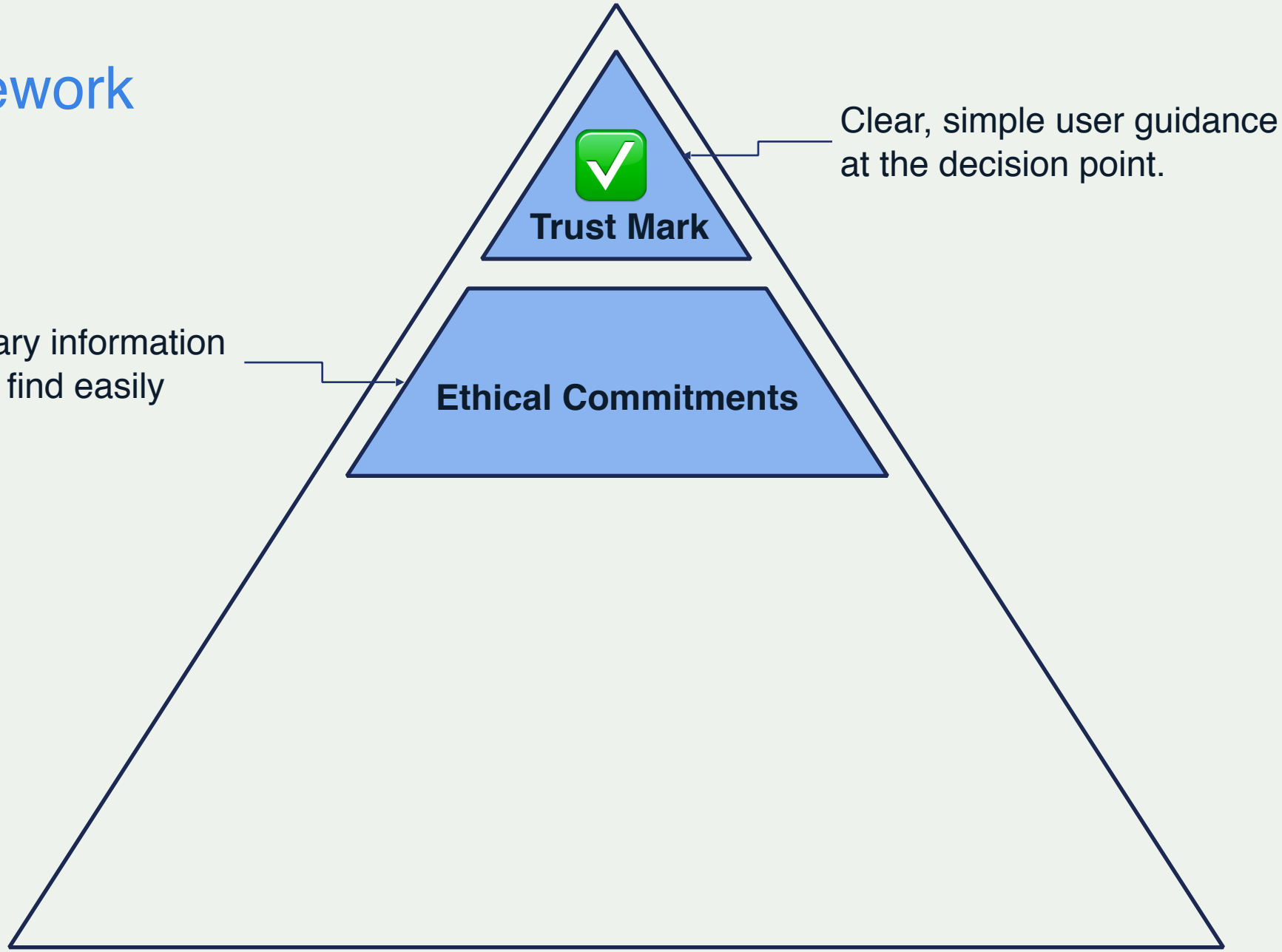
Policy makers:

- Use regulation appropriately
- *Understand that technology is a point solution*

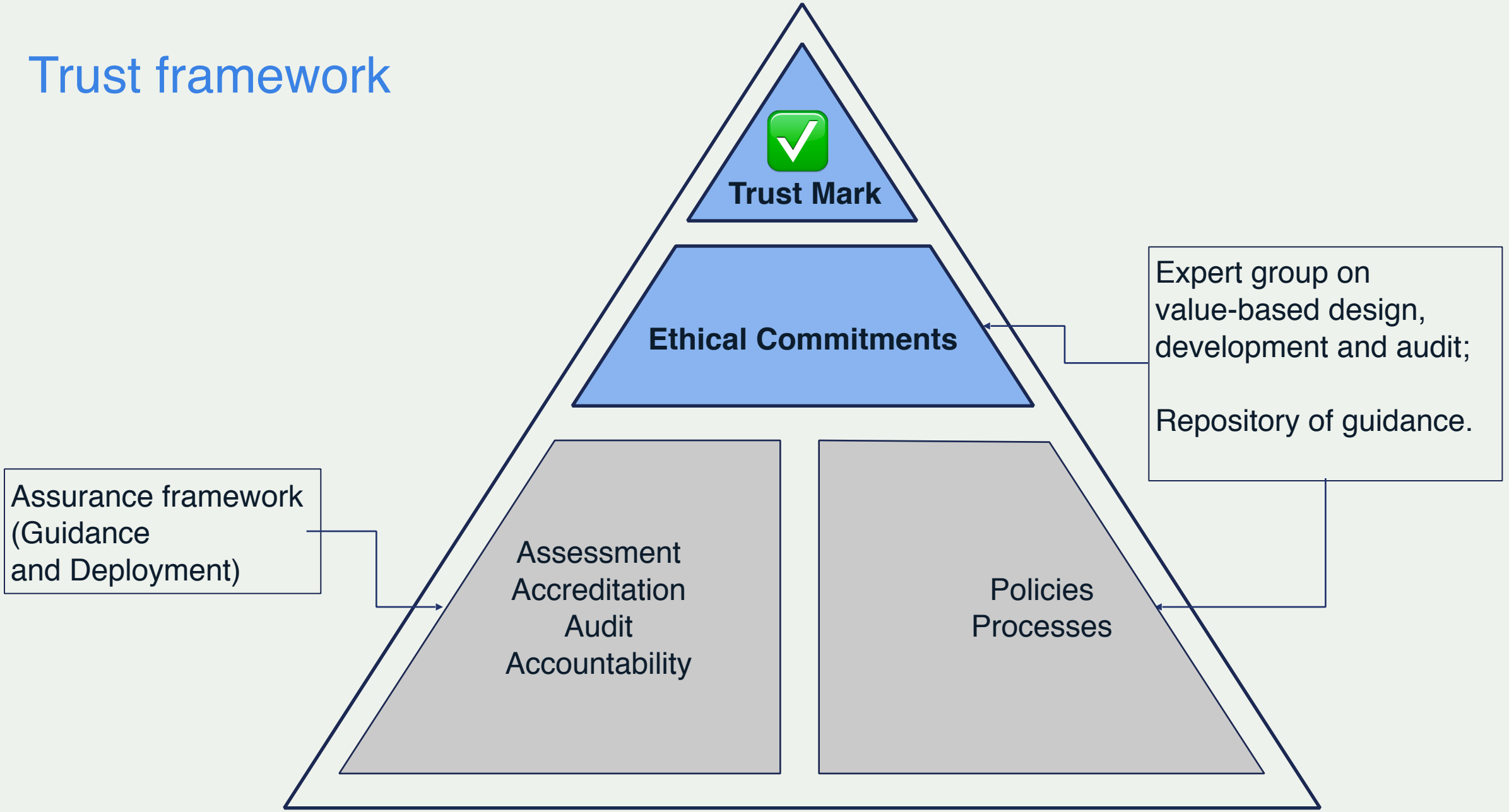
Trust framework



Trust framework



Trust framework

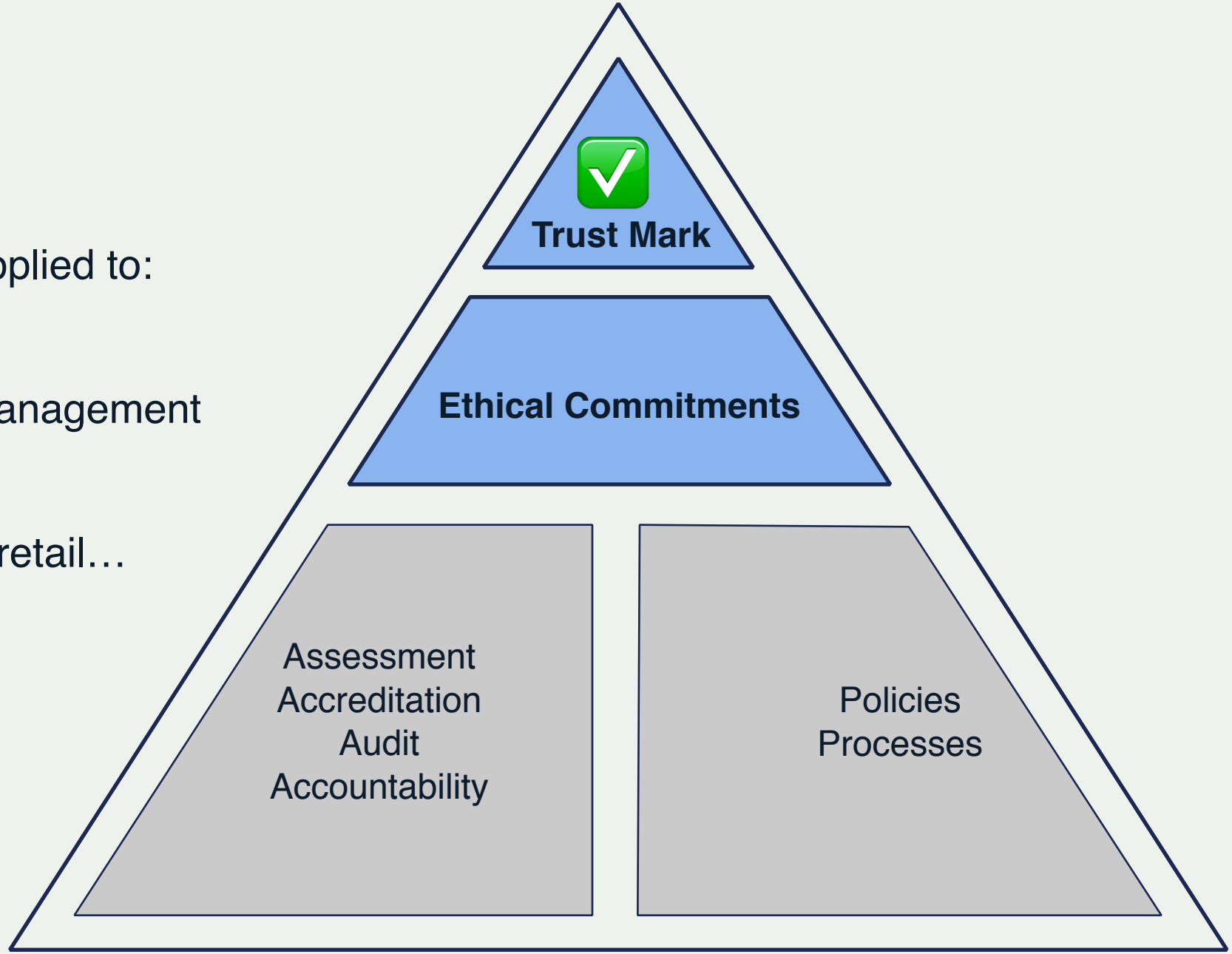


A reusable model

Imagine the same approach applied to:

- Labelling of apps
- Procurement/spplu chain management

- Labelling of IoT devices for retail…



Ethical Data Handling Is The Foundation For Trust.

- Ethical data handling is the foundation for trusted products and services
  - Increases users' confidence in adopting innovation
  - Enriches the relationship with the consumer/citizen
  - Leads to more sustainable economics
  - Makes compliance easier to achieve

Thank you.

Robin Wilton
Technical Outreach Director, Trust and Identity
wilton@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120