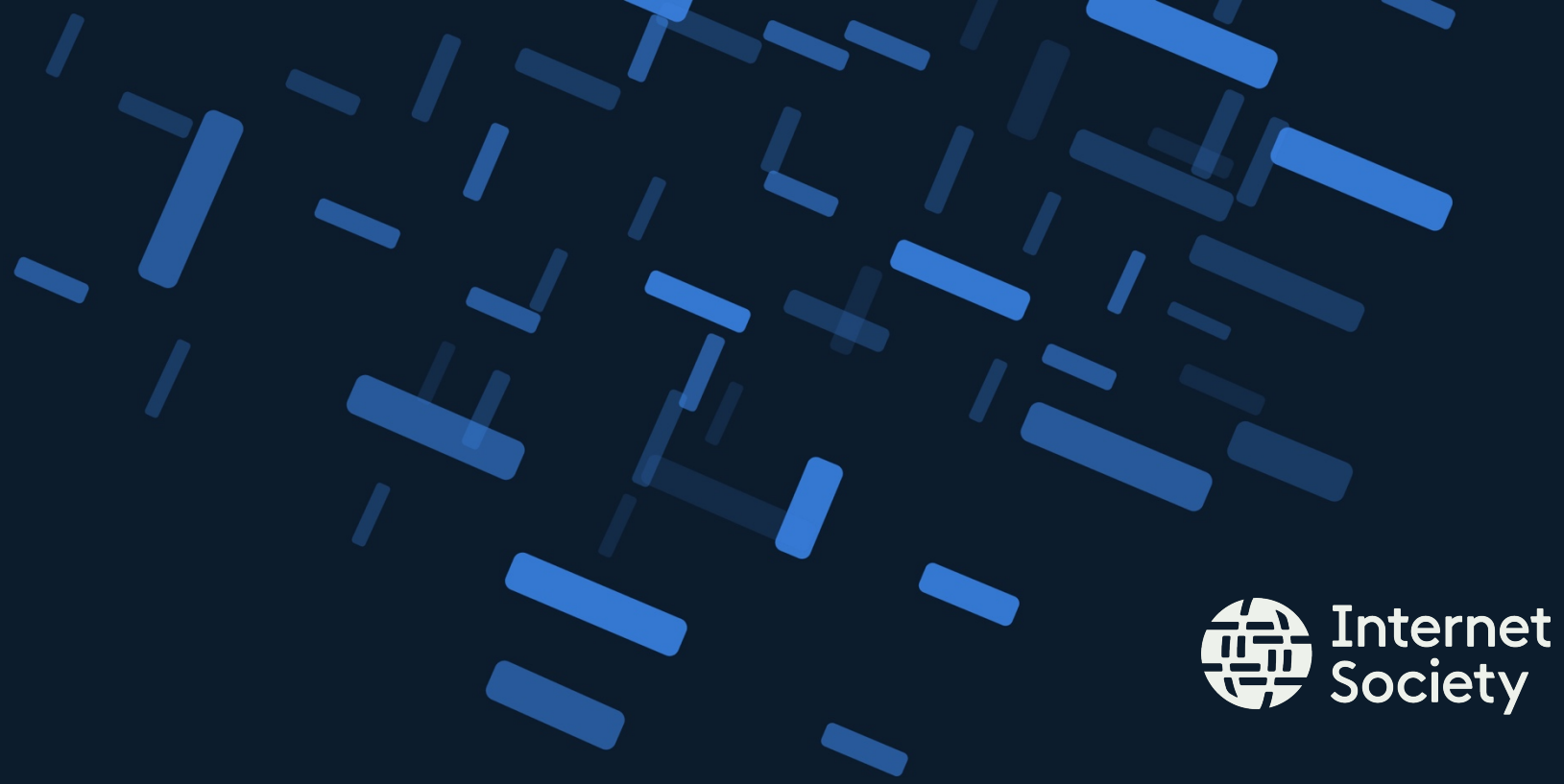


IoT Privacy, Security and Trust

ICTP Trieste,
April 2018

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

ISOC was 25 last year!

Vision: an Internet that is open, globally connected, and secure

Mission: to ensure that the benefits of the Internet reach everyone

Key themes: access, and trust

Global Presence

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

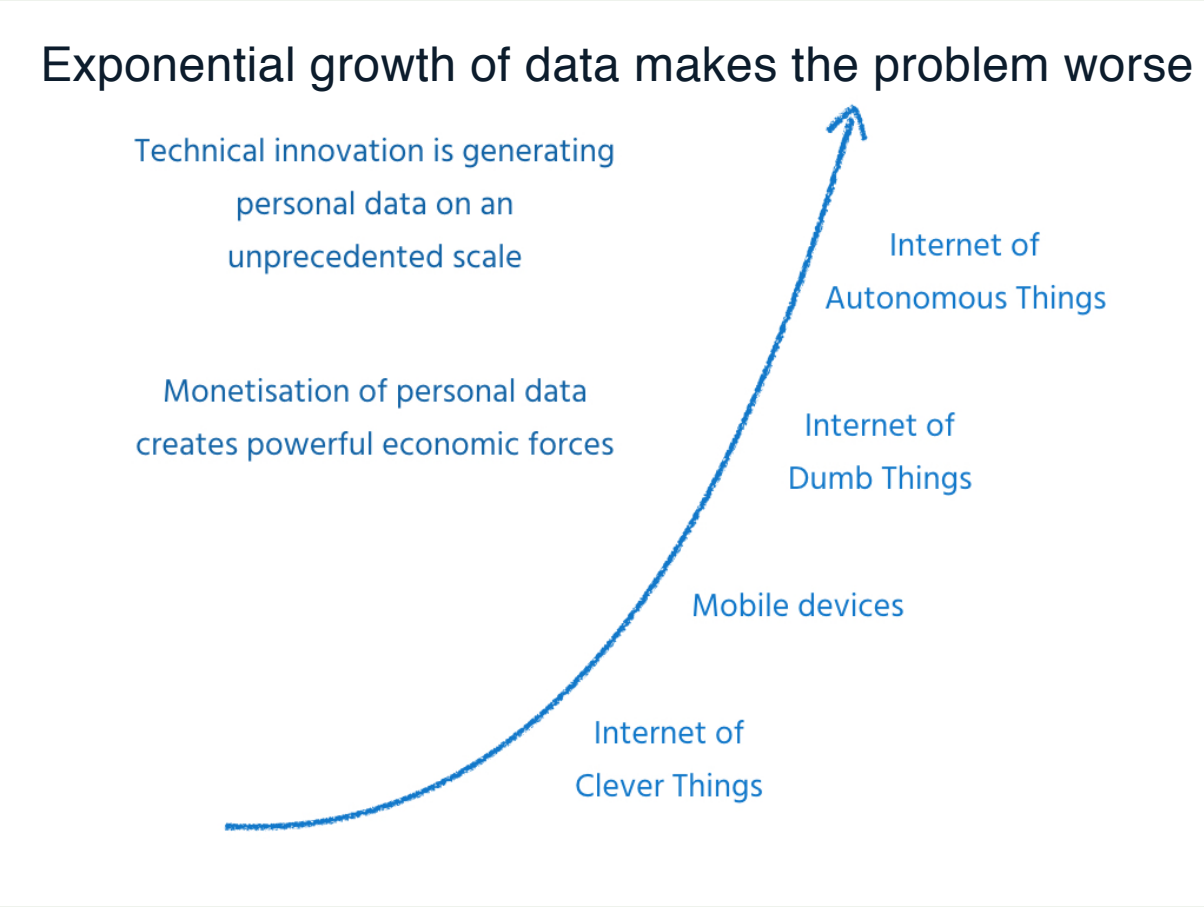
Data protection/compliance is falling short of protecting consumers

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

We're often told we live in the Information Society: we're less often reminded that most of the information is in the hands of others.

Some implications of the IoT phenomenon

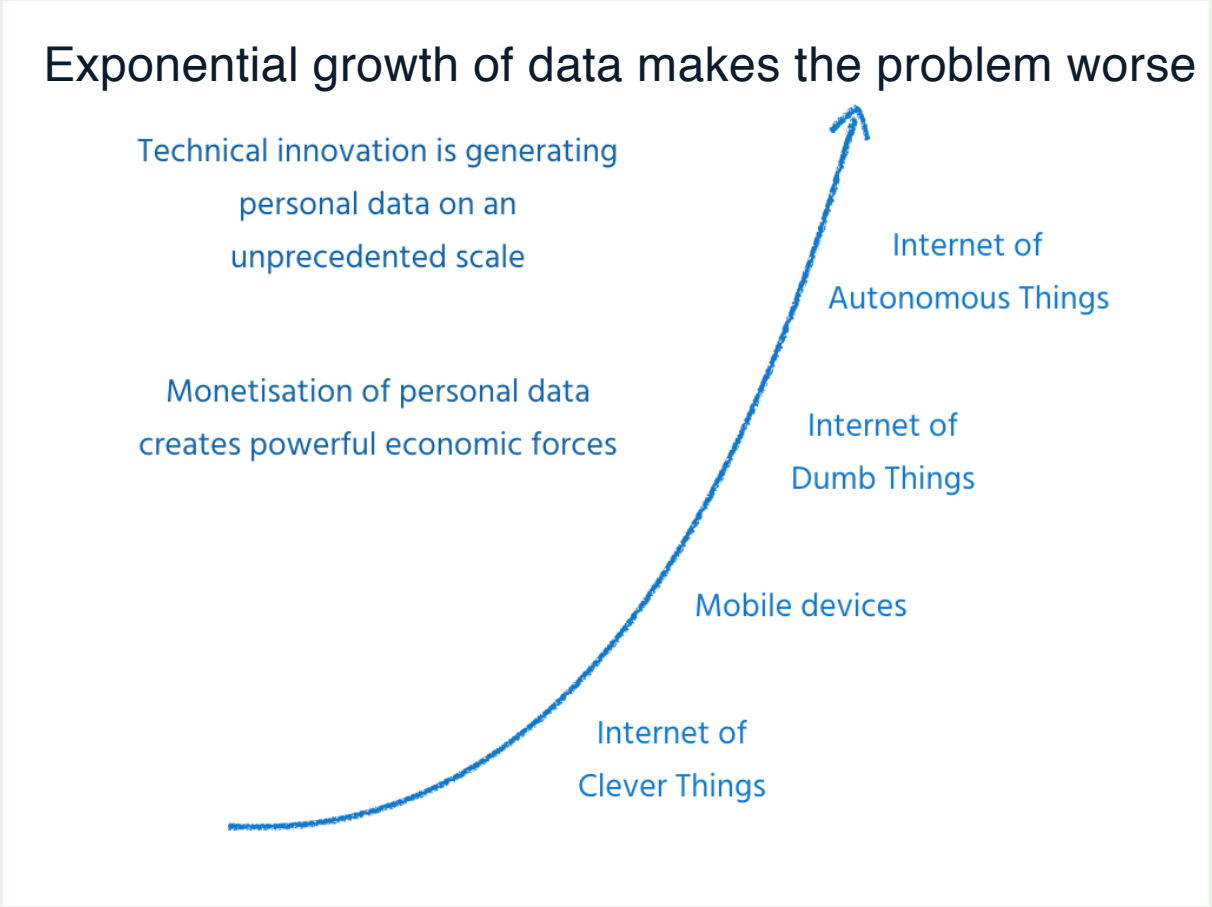
Data growth is (approximately) exponential:

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, so transparency is an issue

- Connected objects, by their nature, collapse contexts and thus challenge privacy (see next slide…)



A Real-World Example from 2016-17

- 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

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

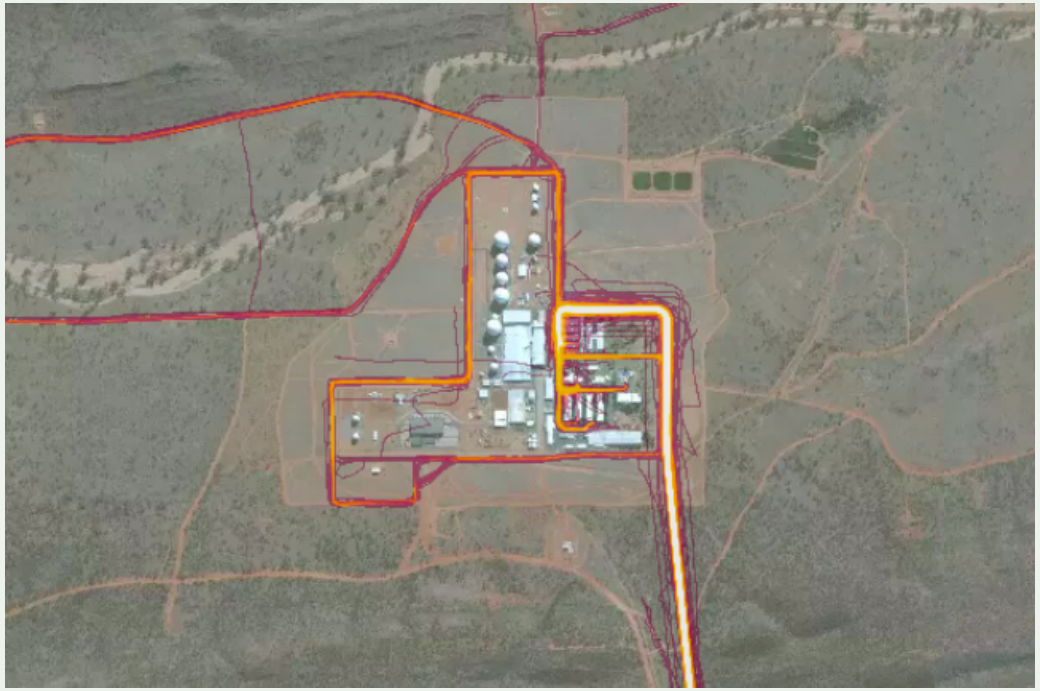
- Values-based design is a viable option: plenty of guidance is available

Some thoughts about sensors and design principles…

First, let's look at unintended consequences.

Things and Contexts

- In the Good Old Days, a stuffed unicorn was just a stuffed unicorn.
- Nowadays, a fitness tracker might personally identify military/intelligence staff.



- Part of the problem, here, is the erosion of “privacy contexts”, without the individual’s awareness, consent or control.

What about sensors… aren’t they simpler?

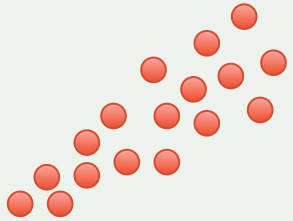
- One sensor gives you a data point (or maybe several): a CO room sensor might also measure CO_2
- CO_2 measurements might allow inferences about human occupancy of the room; CO_2 production data might allow inferences about activity levels in the room.
- All of a sudden, simple sensor data isn’t so binary any more.

(Thanks to IAB Chair, Ted Hardie, for the example)

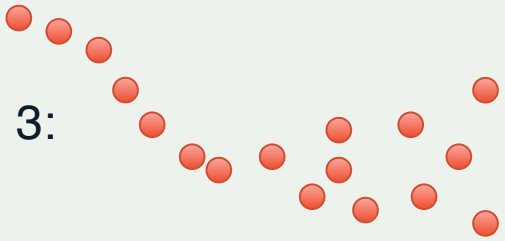
Sensors and mapping data

- Consider these patterns, from a geographically distributed array of sensors (suppose each dot represents a sensor that has registered a noteworthy level of radiation).

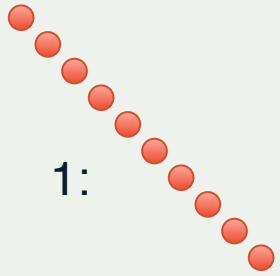
2:



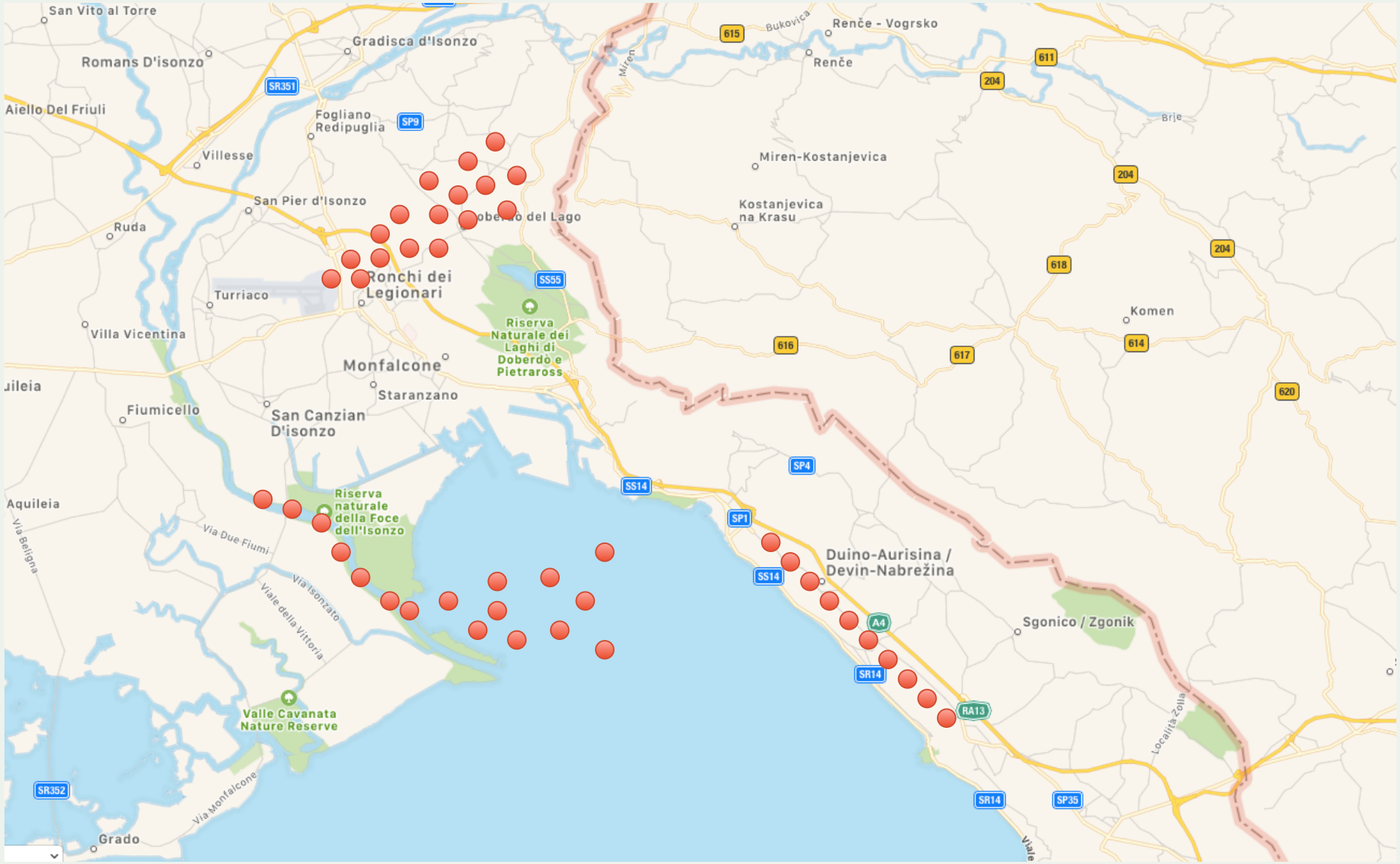
3:



1:



Now let’s plot them on the map.



It’s not so much the data, as what can be done with it

- Inference and correlation change the picture dramatically
- The same data may mean very different things to different people
- Not all stakeholders are focused on the common good (!)

Second, let’s look at some other kinds of consequence.

“Hygiene” and externalities

- Product lifecycles and security functions: are these usually part of the cost-case for an IoT product?
- Are software updates catered for throughout the product lifecycle… including secure decommissioning?
  - Push/pull/negotiated updates… which to choose?
  - Critical update vs critical function/critical timing… how to decide?

- Security failures can give rise to “externalities”: that is, a cost that falls on someone/something other than the one responsible for the failure…
  - privacy
  - Internet availability
  - even the environment

So, how do we decide how to do the right thing?

Embedding values into the design process

- First: recognise that no technology is ethically neutral;
  - It is the consequence of a series of ethical decisions.
- Second: consider consequences, as part of your risk analysis;
- Third: consider principles, as part of your long-term outcomes;
- Fourth: think about “procedural accountability”.

- If you were challenged to produce evidence of how you made the ethical choices you made, could you do so?
- There are good sources of guidance on value-based design

  e.g. “Ethical IT Innovation” - Sarah Spiekermann

Here’s some of what the Internet Society has produced to help…

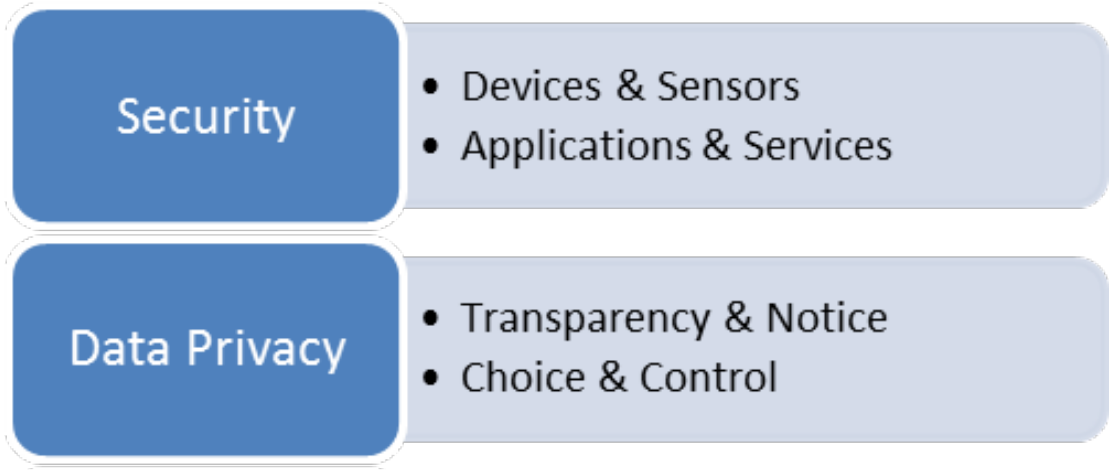
IoT Trust Framework

- Multi-stakeholder working group
- 18 month, consensus driven process

OTA
Online Trust Alliance
an Internet Society initiative

IoT Trust Framework

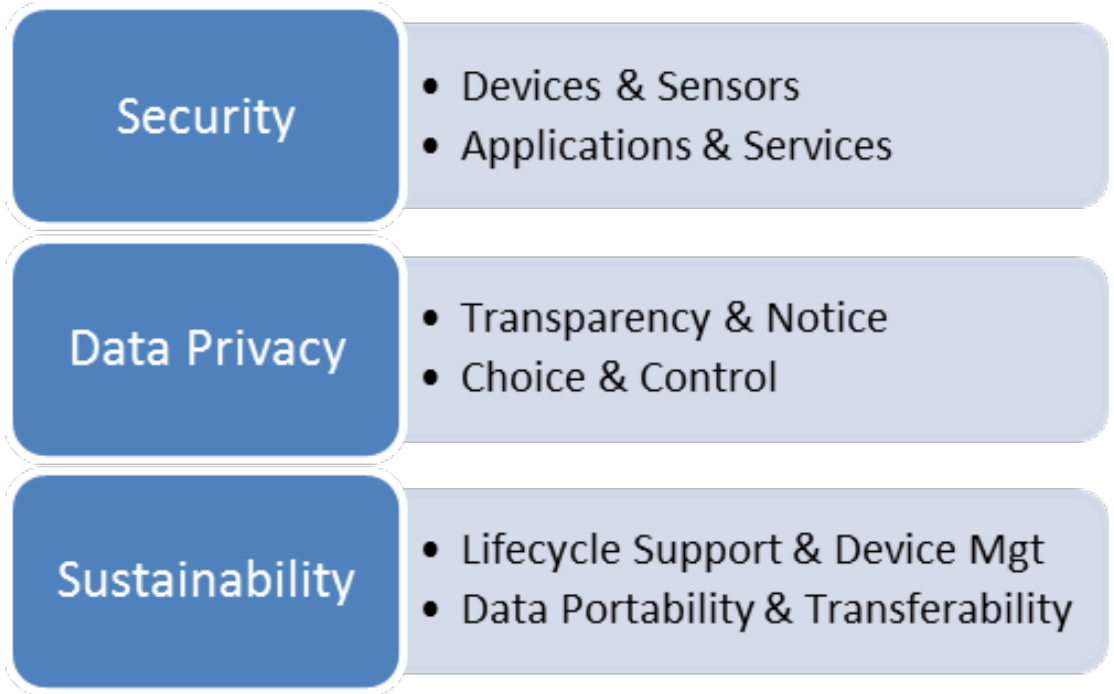
- Multi-stakeholder working group
- 18 month, consensus driven process



Online Trust Alliance
an Internet Society initiative

IoT Trust Framework

- Multi-stakeholder working group
- 18 month, consensus driven process



OTA
Online Trust Alliance
an Internet Society initiative

Evolution

- August 2015 – 93 criteria / principles identified
- March 2016 – v1 released at RSA (30 principles)
- January 2017 – v2.0 released at CES (37 principles)
- June 2017 – v2.5 released (40 principles)

- Latest version posted at https://otalliance.org/IoT

OTA
Online Trust Alliance
an Internet Society initiative

And here’s some of what we are working on in the consumer IoT market…

The Internet Society Calls for an Ethical Approach

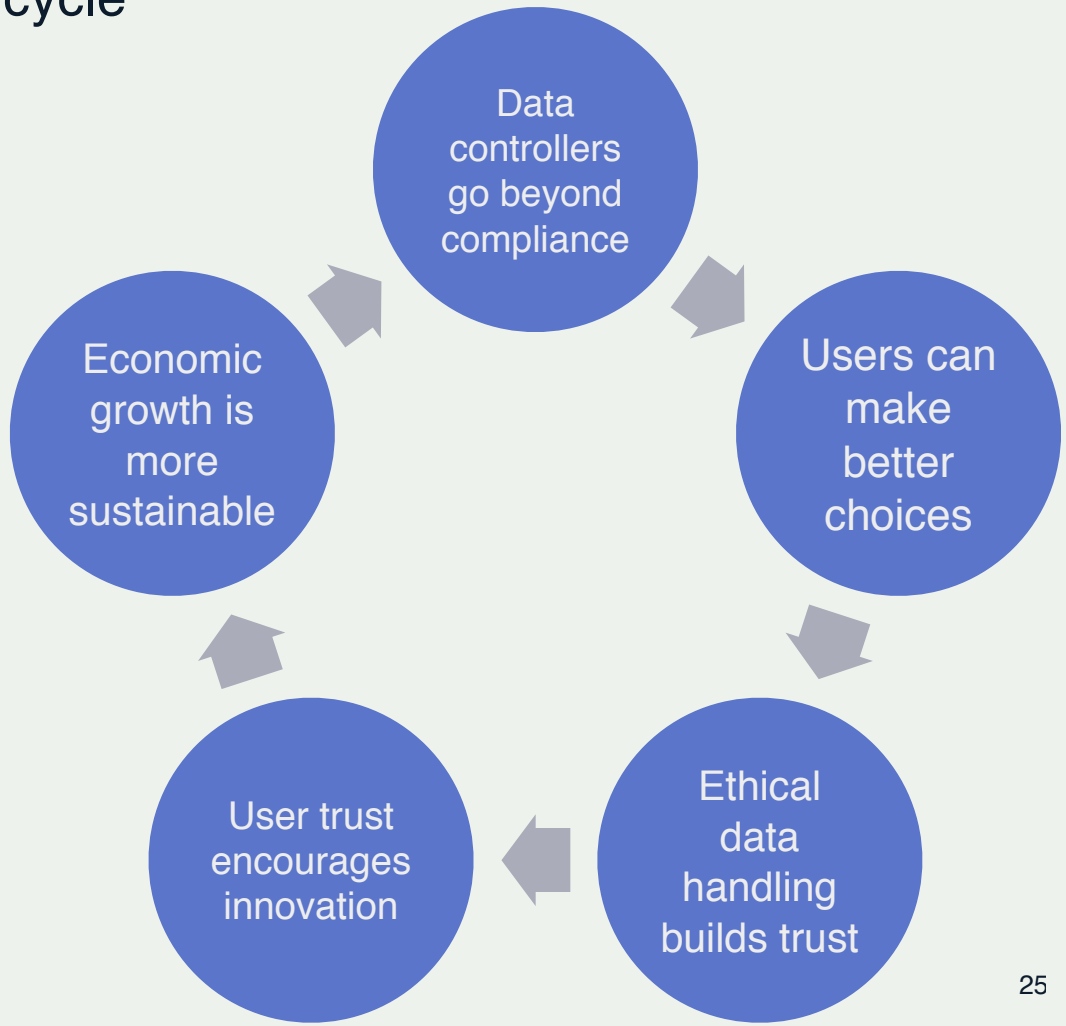
For users:

- 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

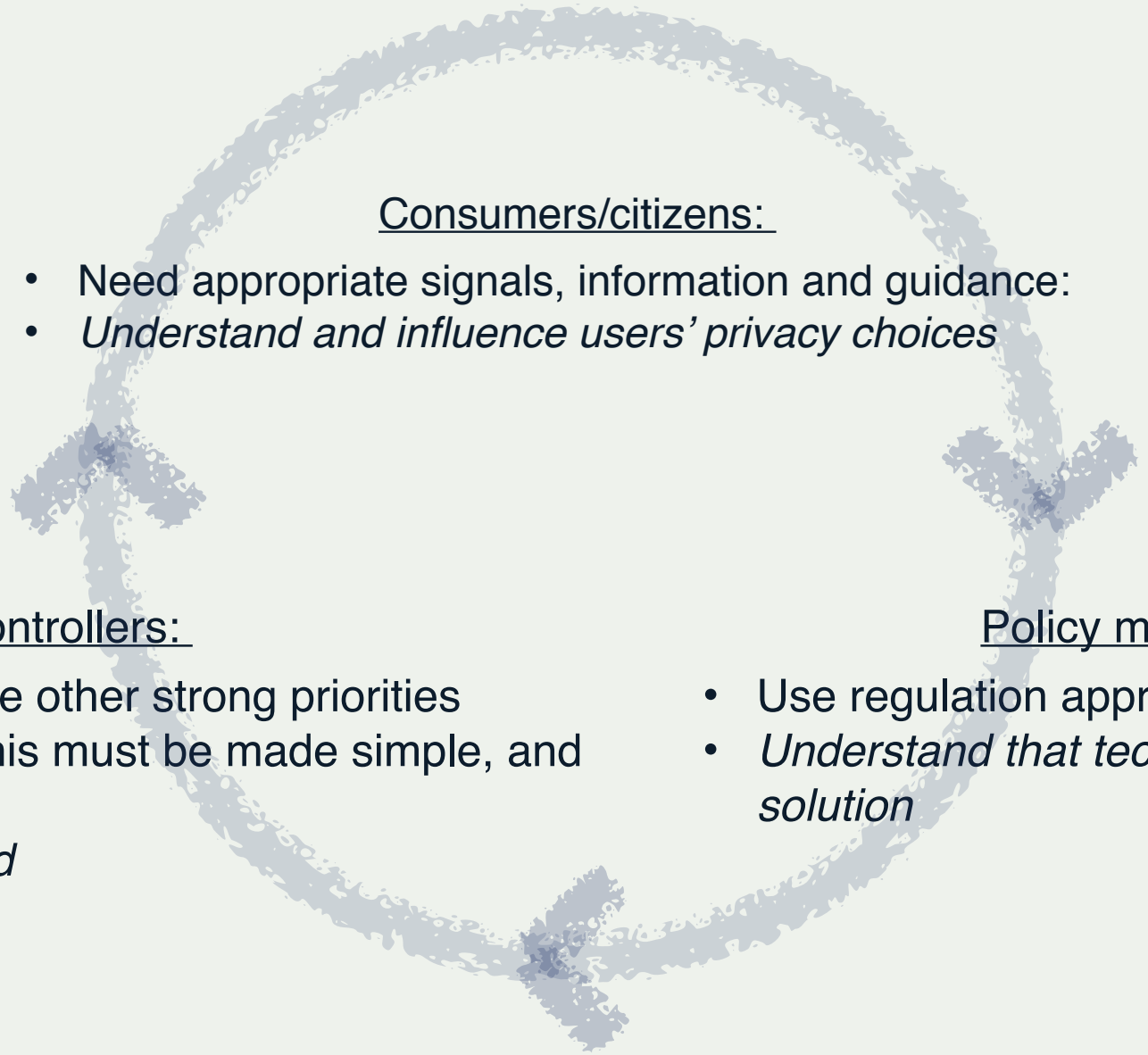
Data controllers:

- 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*

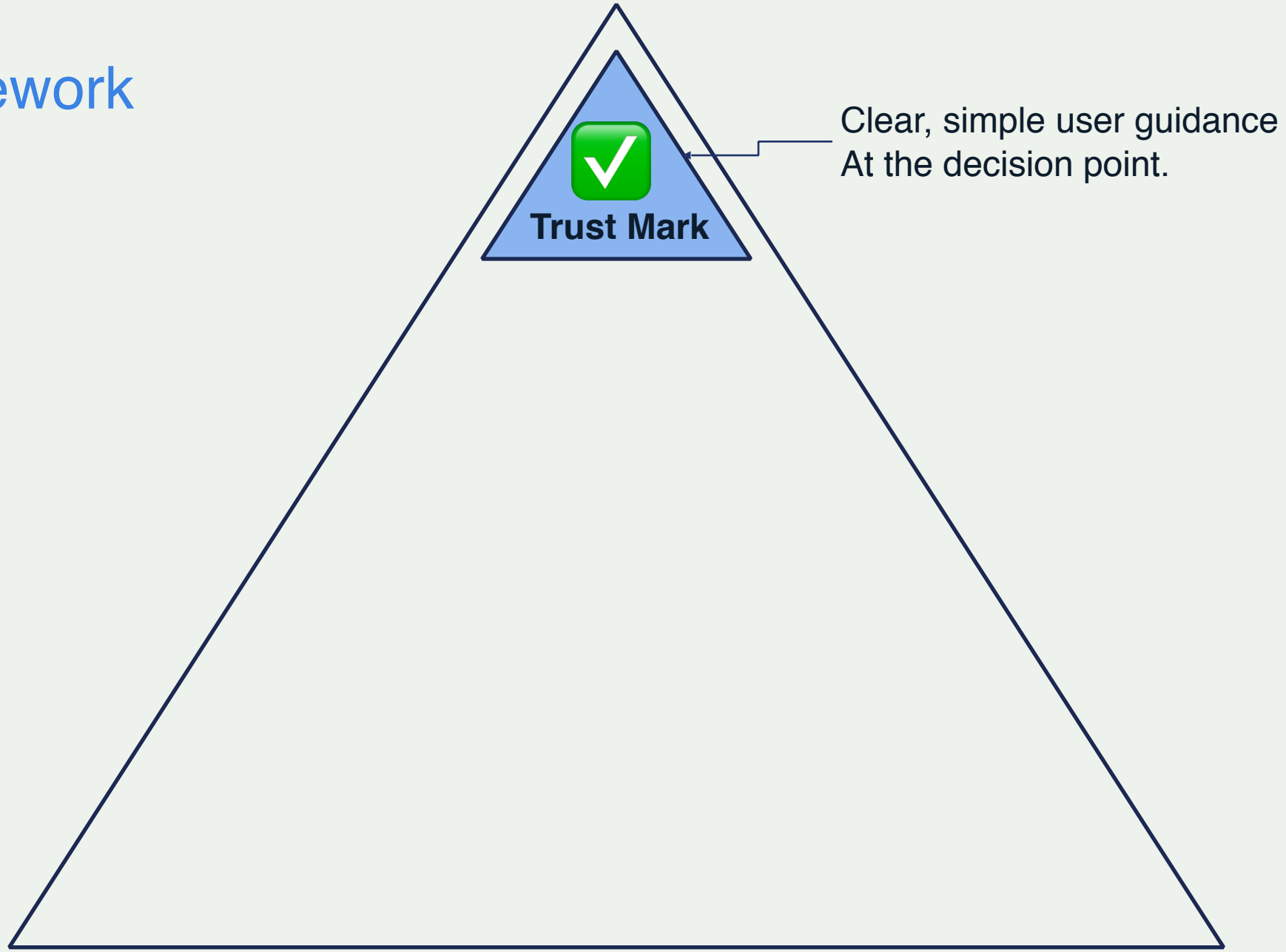
Data controllers:

- 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*

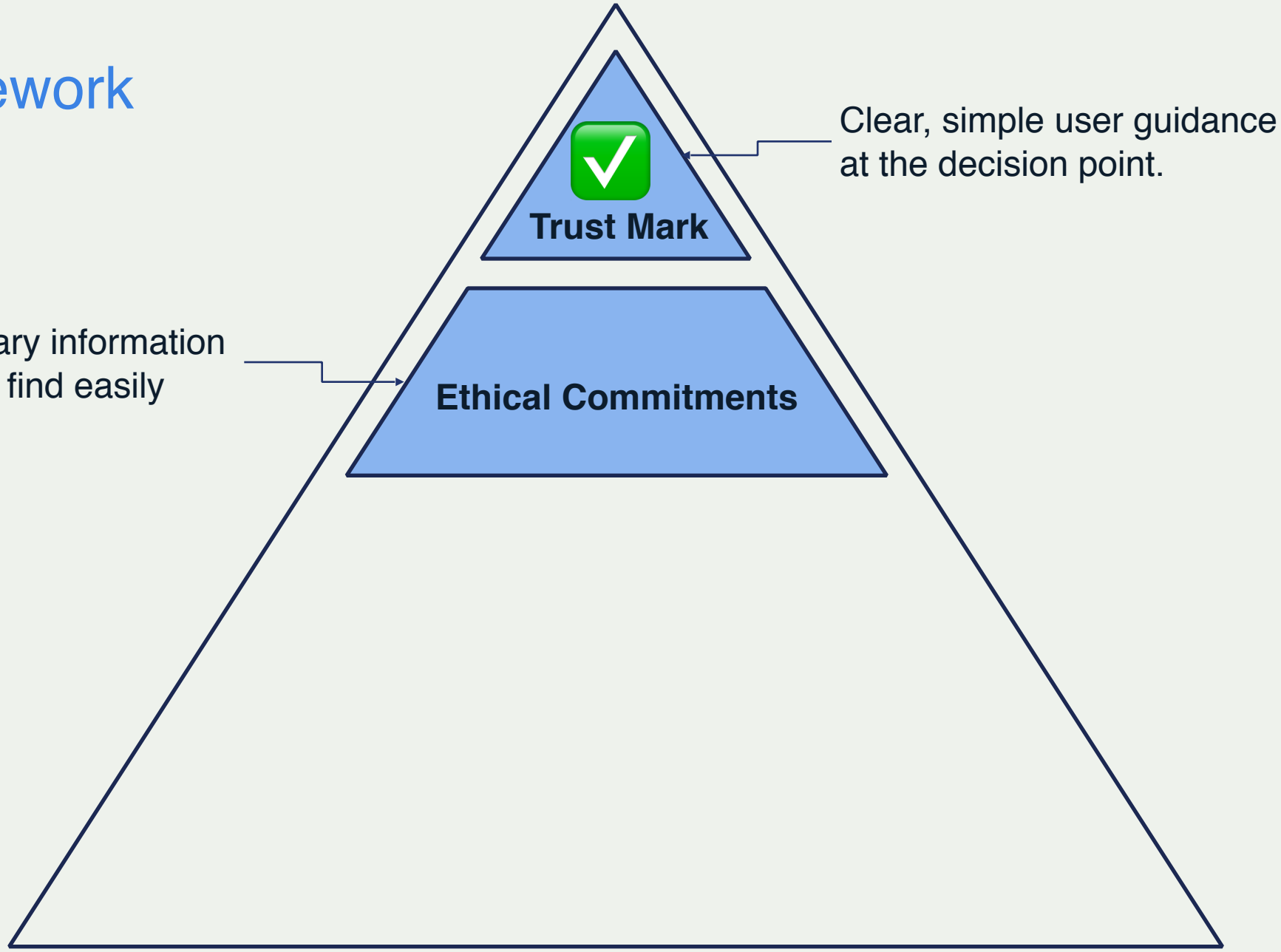
Policy makers:

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

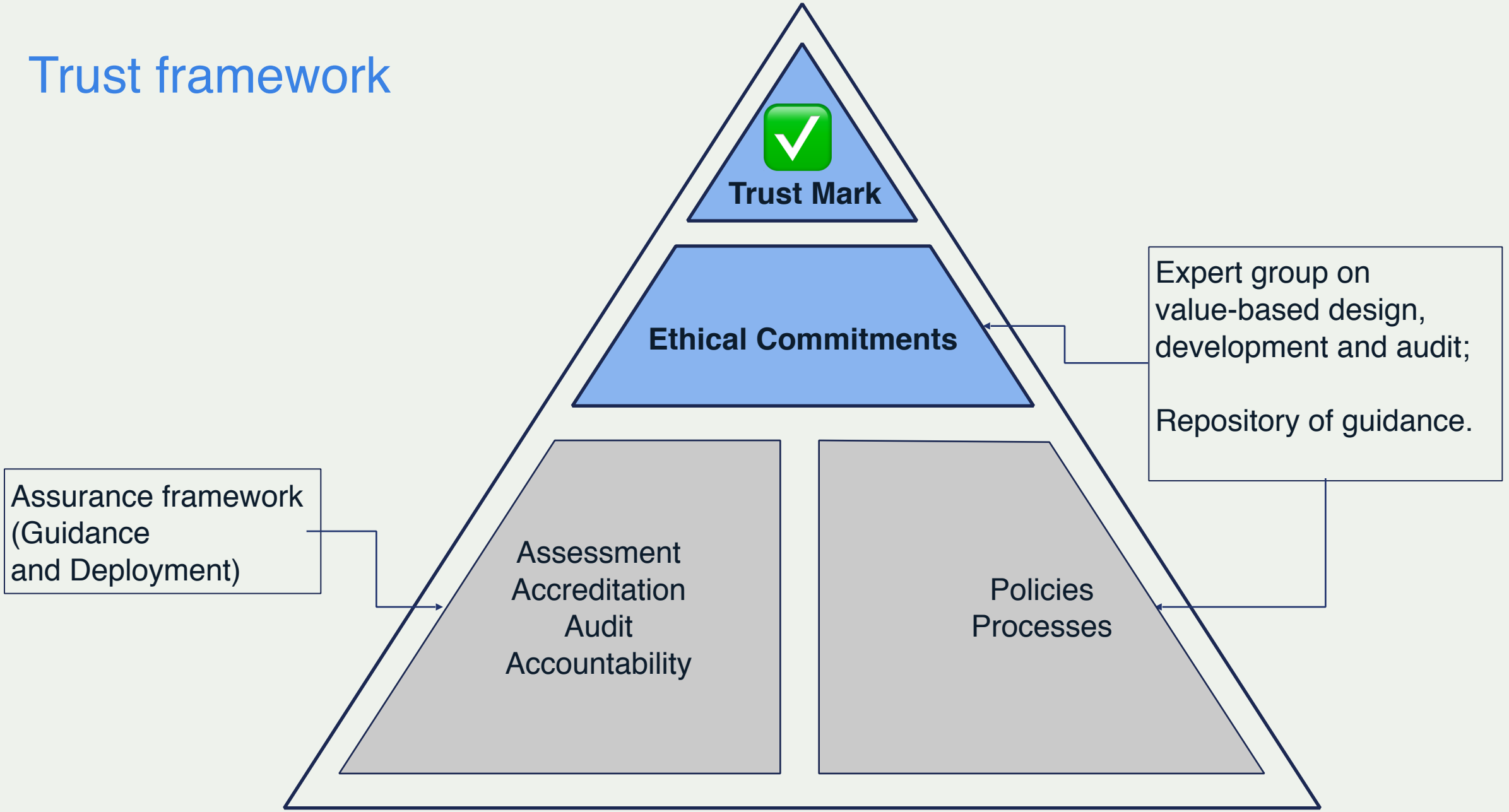
Trust framework



Trust framework



Trust framework

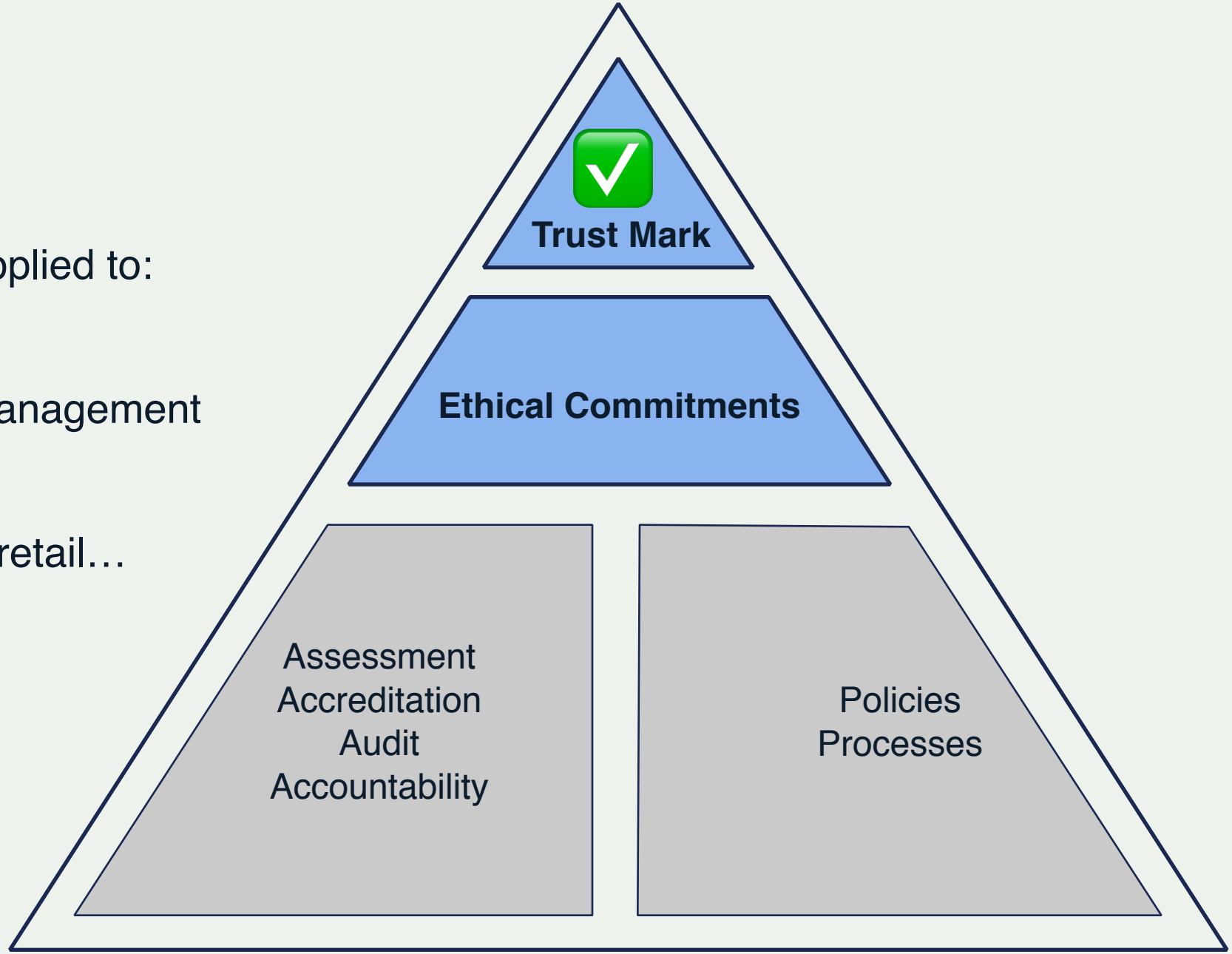


A reusable model

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
@futureidentity

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