Privacy - Principles and Models

MEAC SIG 2021
July 7th

Robin Wilton
wilton@isoc.org

Objectives

We’re all sure we know what privacy and identity are... in practice.

But that doesn’t help us understand them in theory, or how they are related.

In this session, my aim is to:

1. Examine the basic principles of identity and privacy
2. Explain how identity and privacy are related
3. Give you some simple models to understand and explain identity and privacy principles
4. Make some predictions about future areas of risk

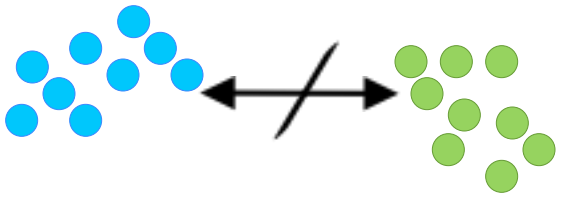
Topics

- What is “Identity”?
- The backward-looking model of identity
- Identities, credentials and attributes
- A forward-looking model of identity
- The “Onion”: how identity and privacy are related
- Practical problems
- Problems of principle

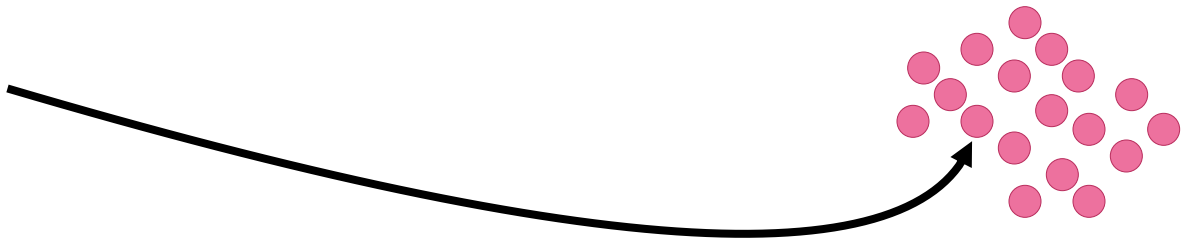
What is “Identity”?

- Philosophically

- Socially



- Administratively



- Technically ... ? We’ll come to that shortly.

- See also: Taxonomy of Privacy - Marit Hansen, Andreas Pfitzmann et al.

Message #1:

Digital identity may be a technical topic, but it should not be left just to the technologists.

A view of identity as “a technical problem, with a technology solution” leads us down a dead end.

When designing identity systems, we should make sure to consider the social and economic perspectives too.

How governments think of identity

- "**Identity** is 'uniqueness in a given population'"
- It is demonstrated by presenting a **credential**
- It is "given to" the individual through a trusted ceremony (Kim Cameron)
- The credential:
    - is "bound to" the individual
    - encapsulates some **attributes** of the individual
    - can be validated when it is presented

- Most of these characteristics are convenient fictions.
- This notion of identity only captures a subset of what it is on the Internet.

How governments think of identity (2)

- This model does have its uses on the Internet - especially when you explicitly want to assert something about yourself (logging in to online banking; paying for something online; accessing your email)

- There is a close relationship between identity and self-determination
- Think about what it would mean not to be allowed a passport, driving license, employer's badge, etc...

- If authentication is mandatory, then access to anything is conditional.

Identity, credentials and attributes

- Technically, an "identity" is an *index to a collection of attributes*
- If you have logged on as "21941508" you must be Lesley Barnes, which means you're in Accounts, so you are allowed access to the invoicing application
- Note how this encompasses authentication, attributes, authorization and access control
- If you are designing an identity architecture, levels of abstraction between identities, user IDs, and indices are a Very Good Idea.

- NB - Plenty of transactions require just an attribute, not identification.
- (For instance, "is over 18")
- Data minimisation is a key principle of Privacy by Design (Dr Ann Cavoukian)

A forward-looking model of identity

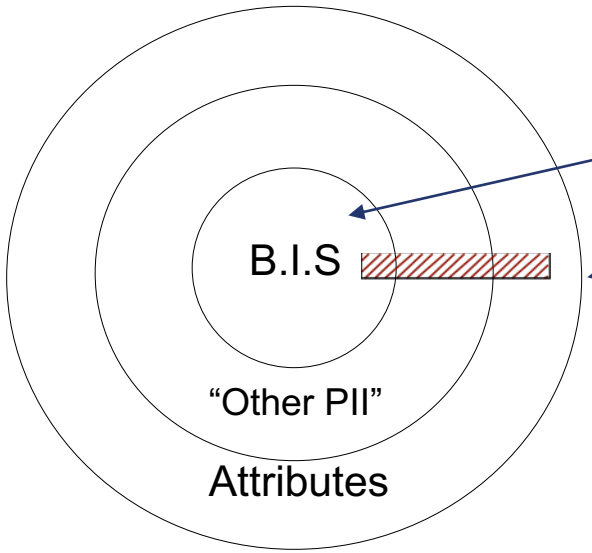
- In human terms, our “identity” is the collection of all our attributes
- *Or* the subset of them we choose to express in a given context
- That subset might or might not include something unique

- If you have enough of someone’s attributes, you don’t need to know who they are…

- This is much closer to the way identity works on the Internet.

Pause for questions/discussion…

How are Identity and Privacy related? (The “Onion” Model)



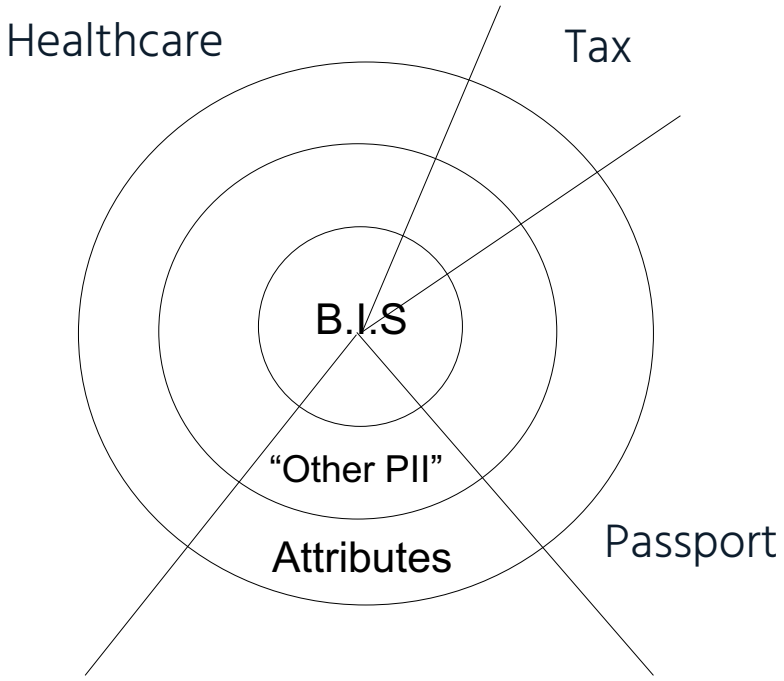
- The BIS (Basic Identifier Set) is what traditionally provides 'proof of uniqueness'
- Credentials usually encapsulate data from multiple 'rings' of the onion

Credentials are not privacy-neutral

- e.g. Using a driver's license to prove your age reveals more than your age;
- By their nature, credentials tend to make transactions 'linkable';
- Privacy-enhancing systems will (must) be better at attribute-level disclosures, or better still, “Yes/No” answers to attribute-level questions.

cf. The UMA project at the Kantara Initiative

How are identity and privacy related?



- A 'segment' of the onion may correspond to sector-specific data (healthcare, tax, employment...).
- Some segments might be 'informal' – such as the separation between your Flickr and email accounts.
- Others, you might want to keep strictly separate – such as online banking.
- One way to look at privacy is as the preservation of "contextual integrity" between sectoral data sets
- See *Helen Nissenbaum, "Privacy As Contextual Integrity"*

It can be unnerving when personal data shows up 'out of context'…

… but innovations and acquisitions erode contextual boundaries (e.g. Facebook and WhatsApp

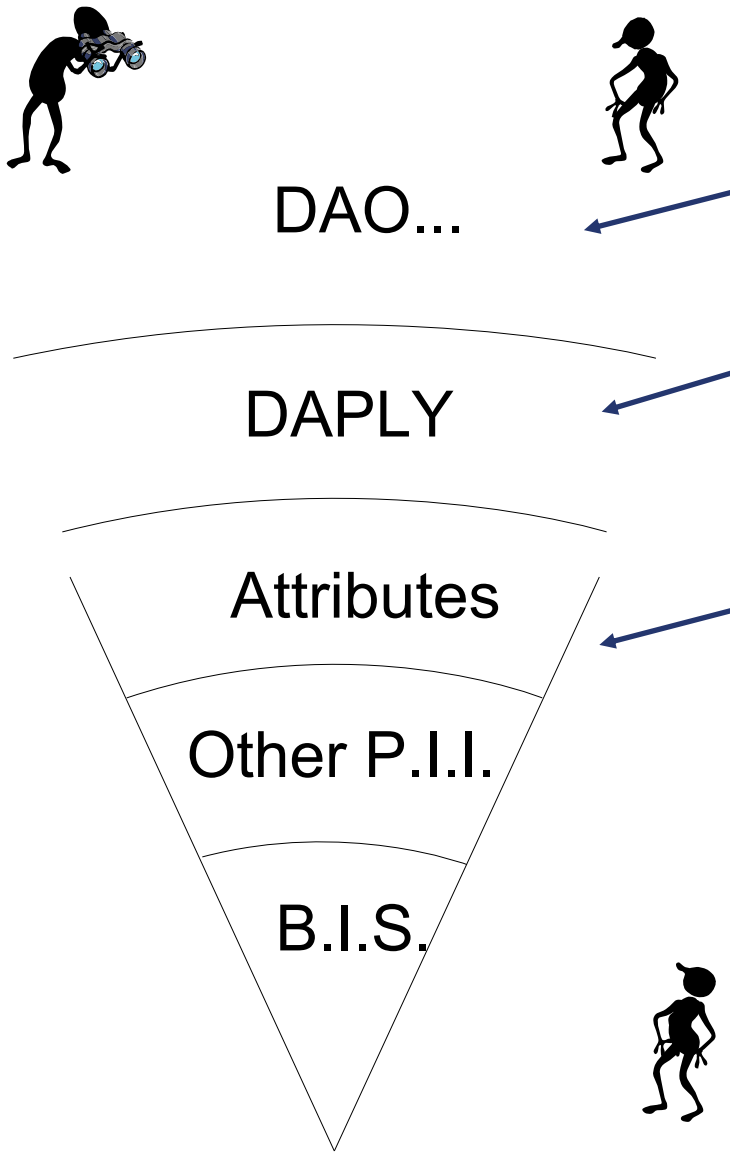
Message #2:

Privacy is about disclosure, but with expectations about context, scope, and purpose.

Privacy is a social/cultural construct.

Technological solutions don’t necessarily fit naturally.

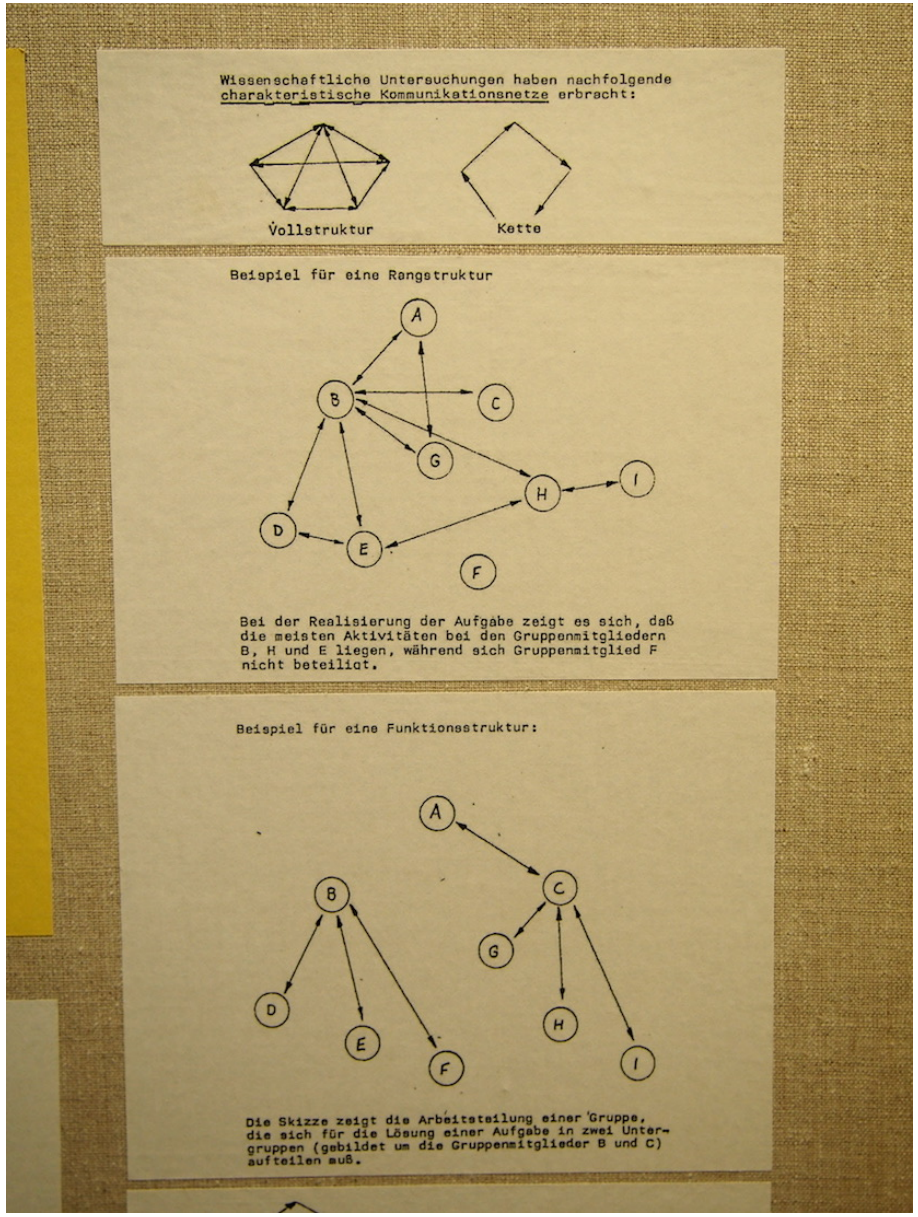
Your privacy isn’t just about you (!)



- **3 - Data About Others**: mass data mining makes third party intervention profitable, even if you don't disclose any PII;
- **2 - Data About People Like You**: if you can be categorised, third parties will apply inferences from other 'group' characteristics;
- **1 - Data About You**: with enough of your attributes, and/or linkability, you can be identified even if you're not asked for credentials.
- Your privacy can be impacted by data about others.

“You don't have to be in the statistics to be affected by the statistics”
(Jason Pridmore, while at Queen’s University, Kingston, ON)

Flawed Perceptions



- The online world sometimes mimics the real world, but it operates by very different rules (and sometimes none).
- “Social Networking” services encourage the user to connive in a fictional reality.
- Users therefore frequently – and willingly - base their behaviour on a flawed perception of risks and the reality which gives rise to them.

Bear in mind that the purpose of most Privacy Policy Statements is to limit service providers' liability, not to ensure better privacy outcomes for the data subject.

Image: study of de facto communication networks among citizens.

Source: Stasi Museum, Leipzig:

Message #3:

Flawed perceptions lead to flawed decisions.

If we don’t think our privacy is at risk, we’re unlikely to think about protecting it.

In the current online environment, we may have little option:

think about the opportunities you have to exercise choice and agency…

What is it, in the system, that allows you to express and enforce your privacy preferences?

Practical next steps

- Privacy is
  - A social overlay
  - On a data-sharing ecosystem
  - Which has many stakeholders
  - With diverse relationships of power and money
  - Each operating in their own “context”

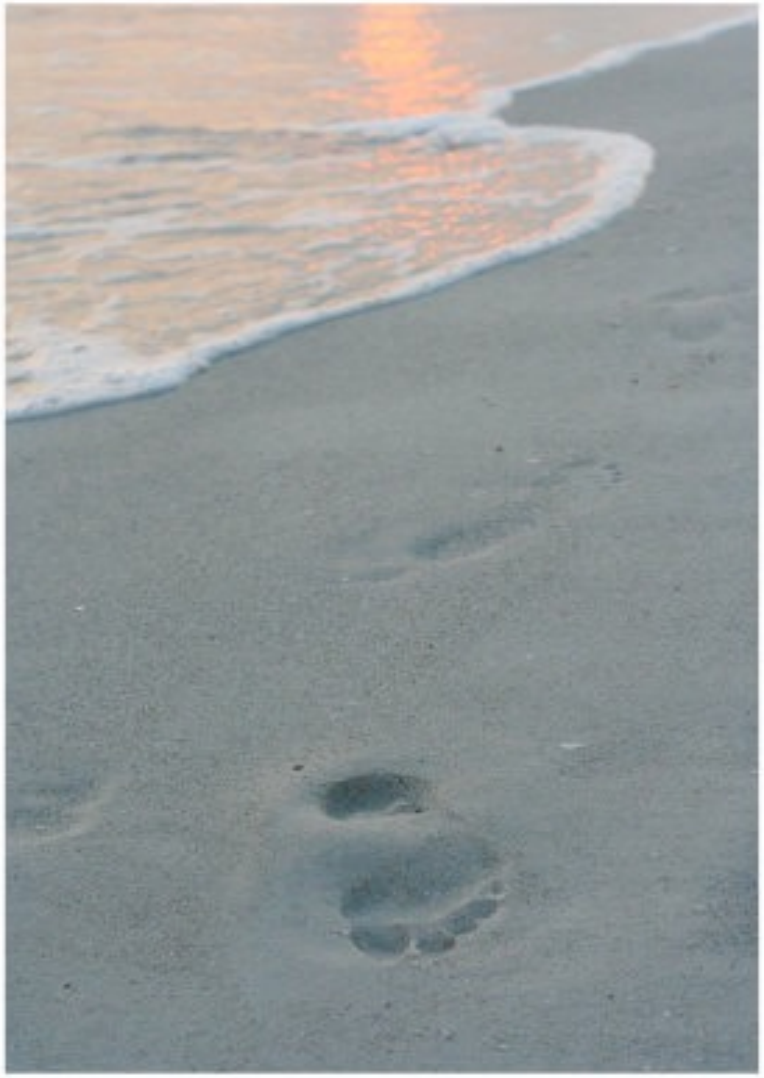
- Fit technical mitigations into a holistic approach, with legal, compliance, policy and cultural measures;
- Remember that *ultimately*, what you are trying to control is not data, but the use to which that data is put... which is a human problem, not a technical one.
- Does what you are building increase user agency, or reduce it?

Pause for questions/discussion…

Supplementary topic

How much do we really understand about personal data?

Have you seen your digital footprints lately?

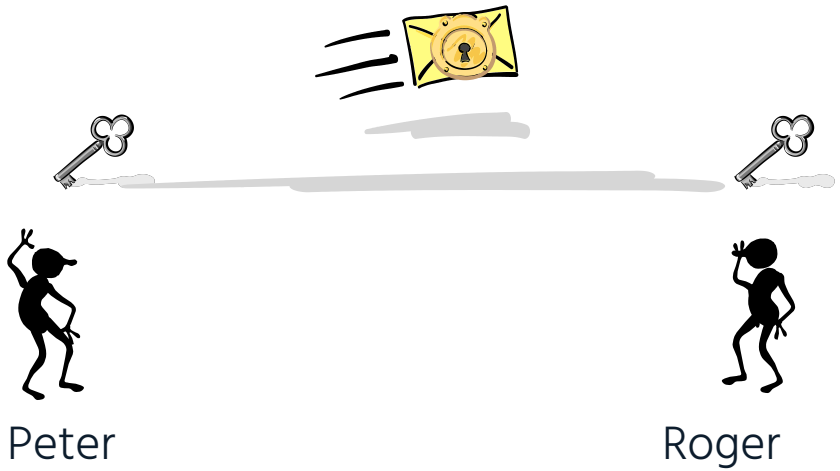


- Much of our online behaviour is based on flawed perceptions about risk
- Few of us appreciate how much data we disclose (and IoT represents a massive increase)
- Even fewer understand the complex ecosystem of data-sharing which (currently) funds so many online services
- (cf. Sarah Spiekermann and Wolfie Christl - Networks of Control)

- The user experience often deliberately says nothing about privacy

- It is hard to manage something you can't see

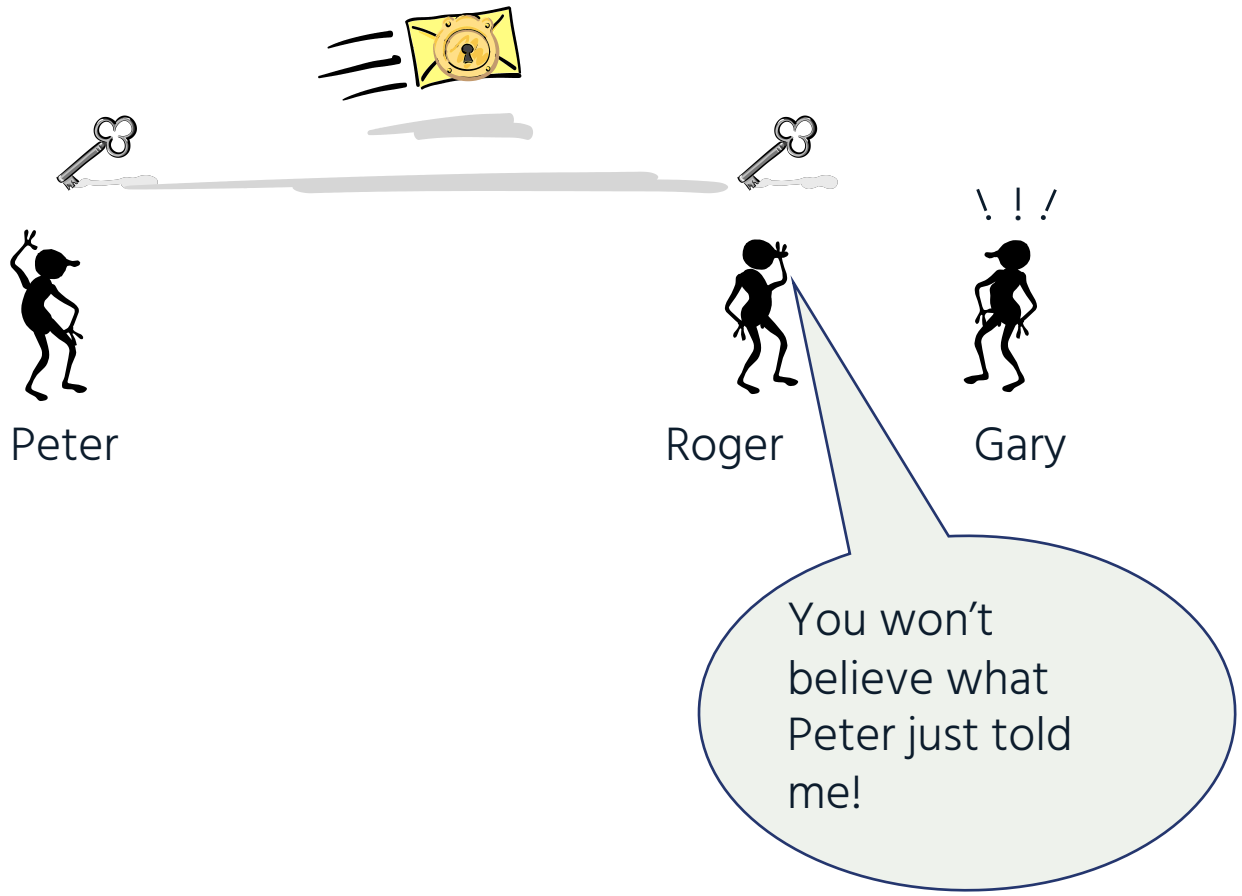
Technical protection has limits



- Privacy is not about secrecy, but about controlled, contextual disclosures
- If Peter sends Roger an encrypted letter, he still wants Roger to see the contents
- Encrypting the letter protects it as far as Roger
- To see the contents, Roger must be able to remove the technical protection applied by Peter: Roger must have the key.

At that point, Peter's privacy is no longer protected by technology.

Technology is only ever part of the answer

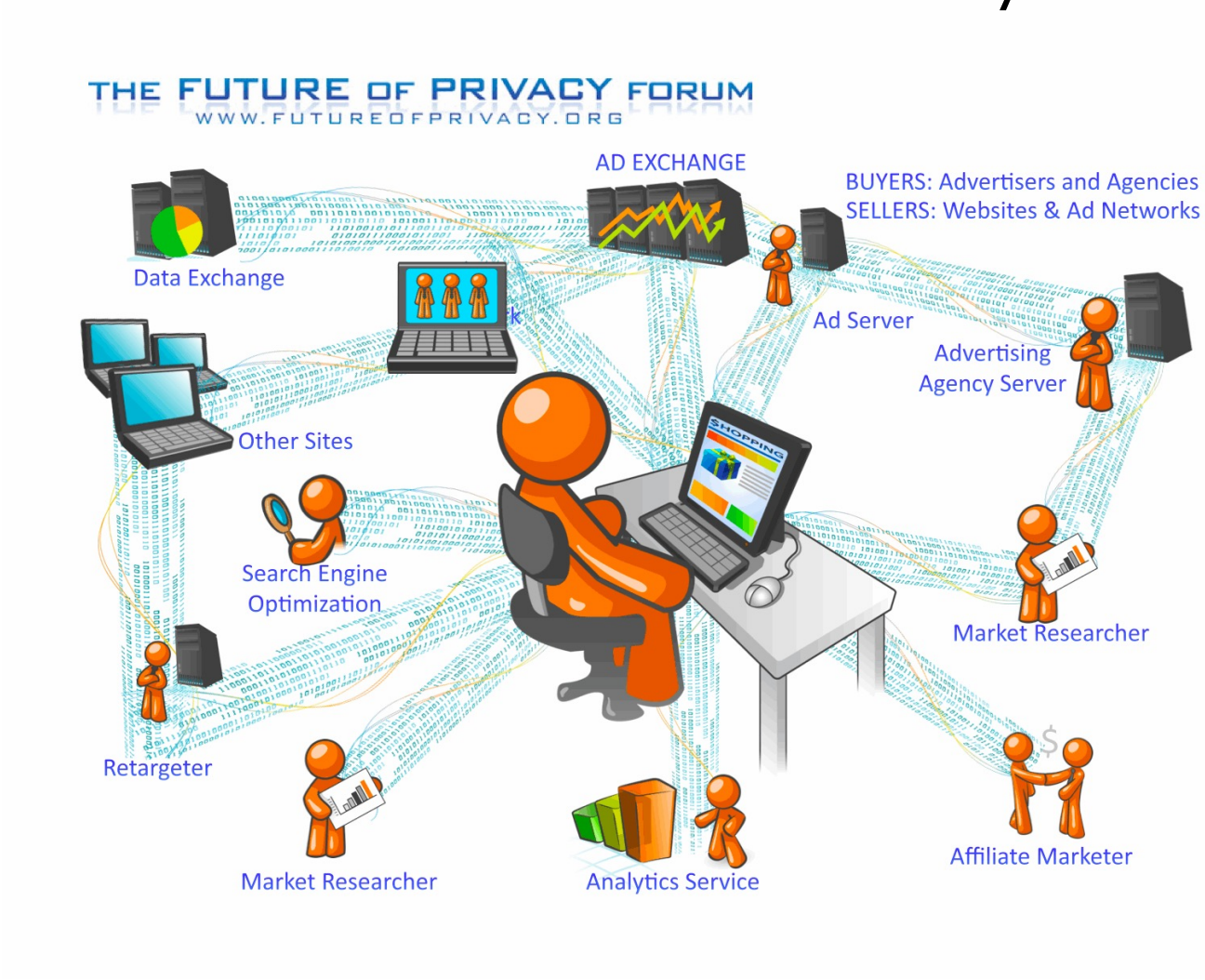


- Privacy is not about secrecy, but about controlled, contextual disclosures
- If Peter sends Roger an encrypted letter, he still wants Roger to see the contents
- Encrypting the letter protects it as far as Roger
- To see the contents, Roger must be able to remove the technical protection applied by Peter: Roger must have the key.

At that point, Peter's privacy is no longer protected by technology.

- *(Ultimately, this is not a technical question about the exchange of data; it's a social question about the transfer of knowledge)*

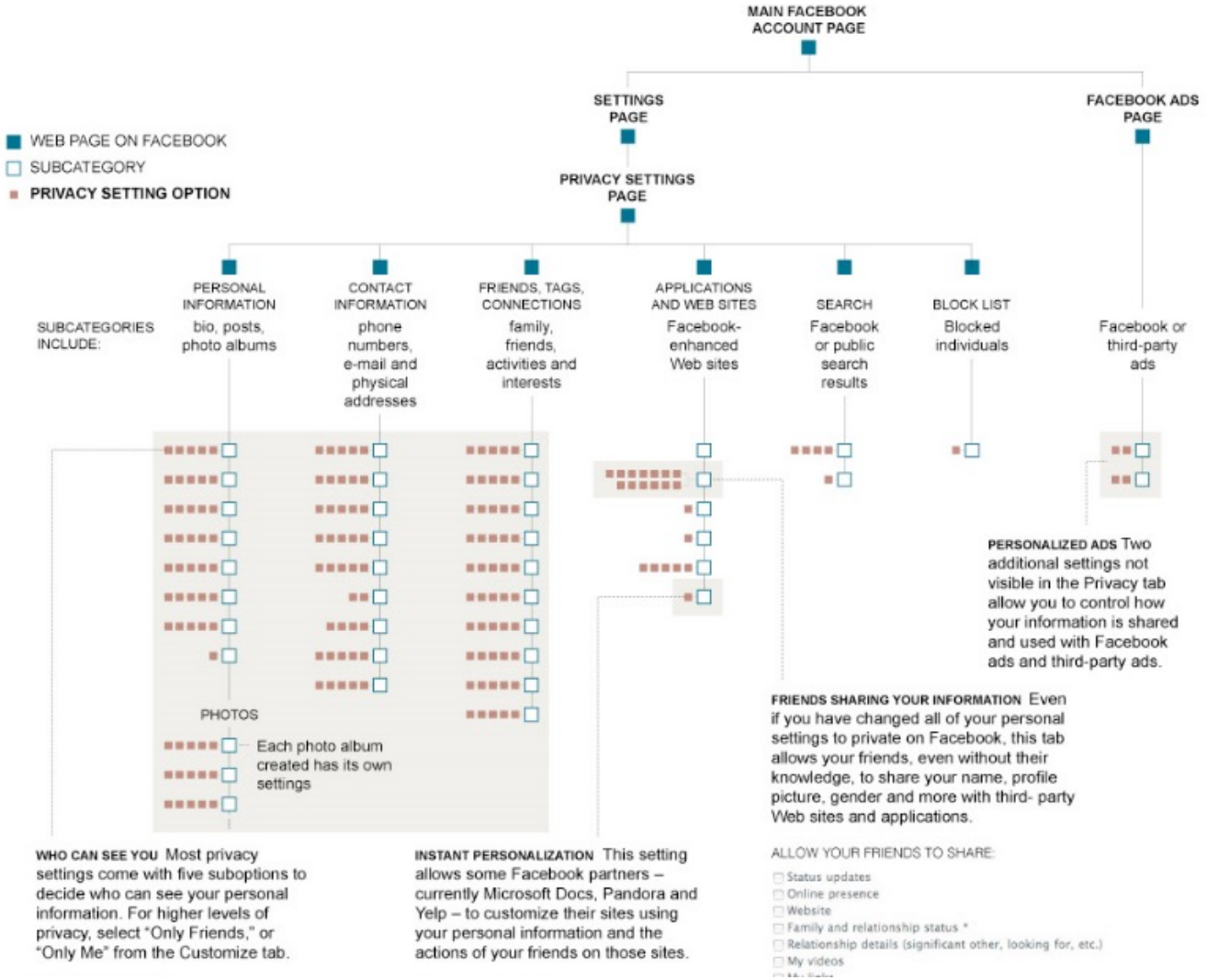
The monetisation ecosystem



Source: Jules Polonetsky, Future of Privacy Forum
http://www.futureofprivacy.org/2010/04/29/before-you-even-click/

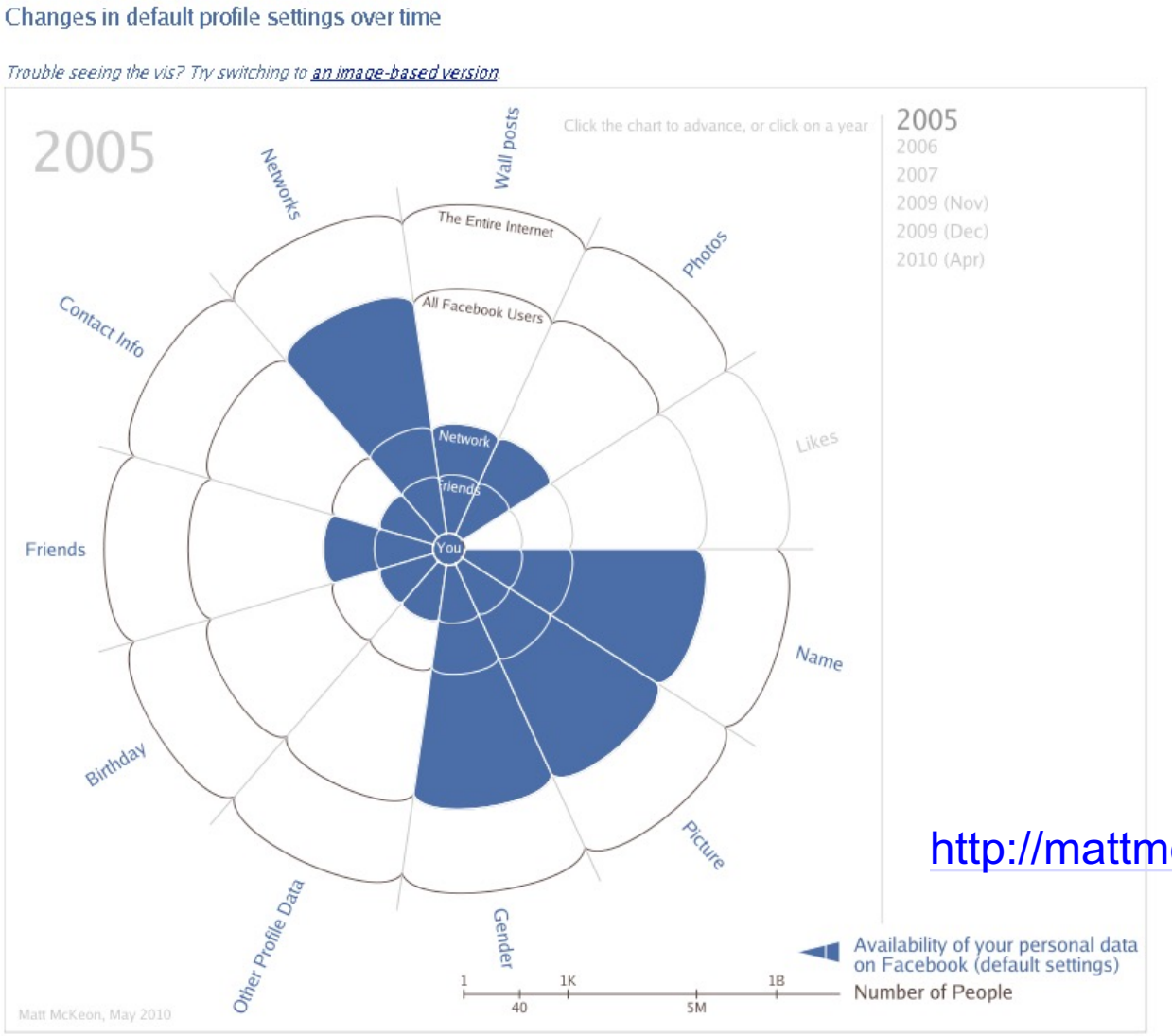
Meaningful Consent and Control:

2010 – Facebook's "Bewildering Tangle"



Meaningful Consent and Control:

Matt McKeon's much more elegant visualisation



http://mattmckeon.com/facebook-privacy/

Privacy Myths (and Mythunderstandings)

"If you've nothing to hide, you've nothing to fear..."

- I should not have to tell my doctor my bank balance, or my bank manager my weight!
- (And can I have your PIN, please…?)

"Privacy is about keeping your data secret"

- Privacy is not secrecy: it is disclosure... in a context.

"Privacy is about data ownership: I should own my data"

- This is not about "your" data; privacy is about rights over information which could affect you.

"Technology is the solution"

- Privacy is a social construct: technology can only ever be a part of the solution.

"Privacy as a social norm is a thing of the past"

- This is nonsense, yet it's the philosophy of a very powerful company.

What these myths have in common is that they play down the value of your privacy, and the nature of information which can degrade it.

Thank you.

Robin Wilton
wilton@isoc.org

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

Rue Vallin 2,
CH-1201 Geneva,
Switzerland.

11710 Plaza America Drive
Wiehle Avenue,
Reston, VA
20190-5108 USA.