Token-Based Consent Management to Support Data Subjects' Rights

Chris Cooper
Know Now Information

Richard Gomer **m.c. schraefel**
University of Southampton

Consent

consent =

a genuine

choice +

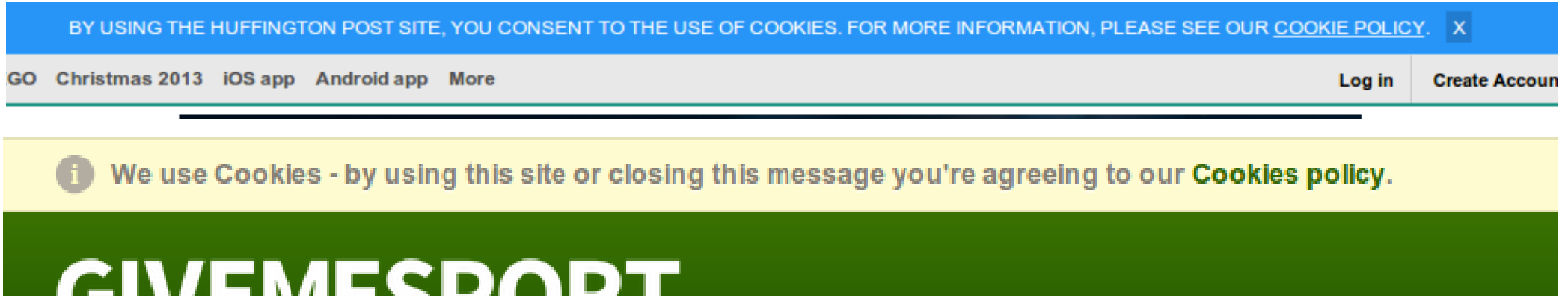
understanding

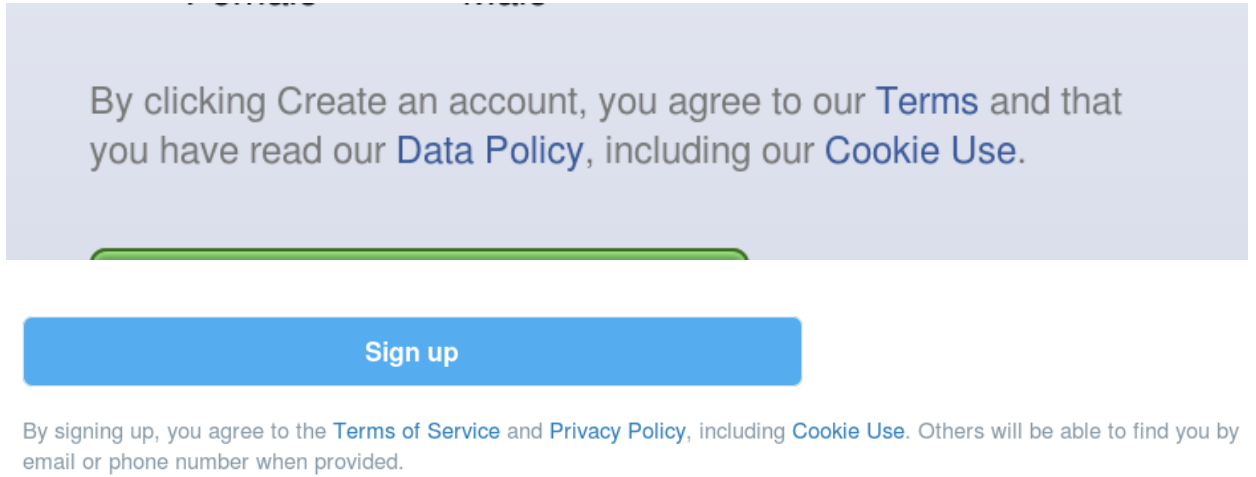
of the implications

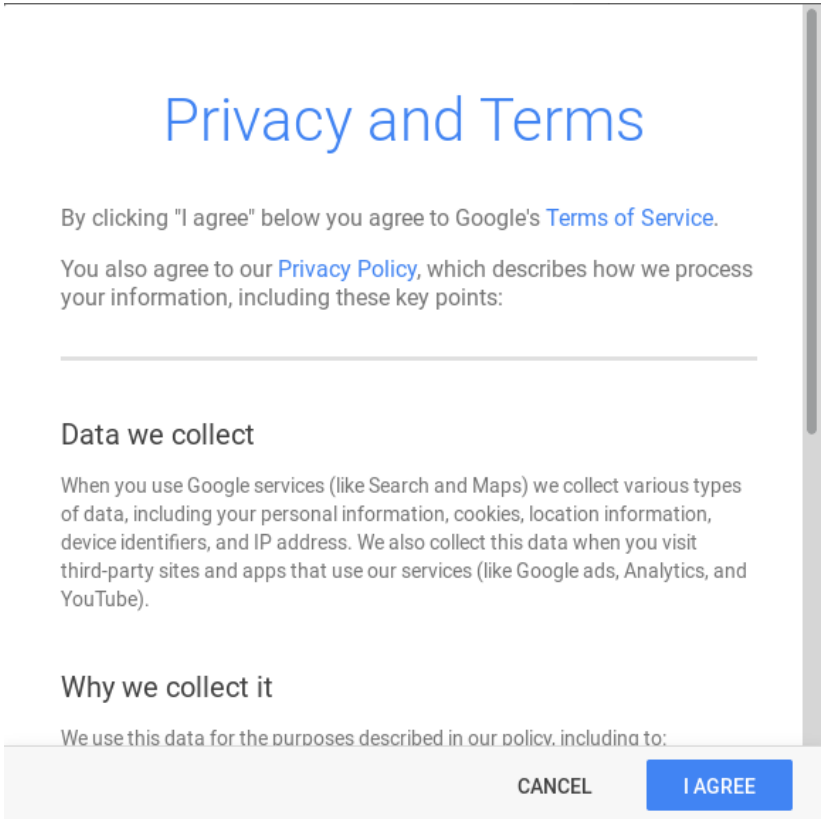
Consent

a genuine
choice +
understanding
of the implications
= consent

Notice and Consent







Consent + Interaction

- Consent is transactional, it necessarily involves multiple parties
- Consent is an **interaction problem**

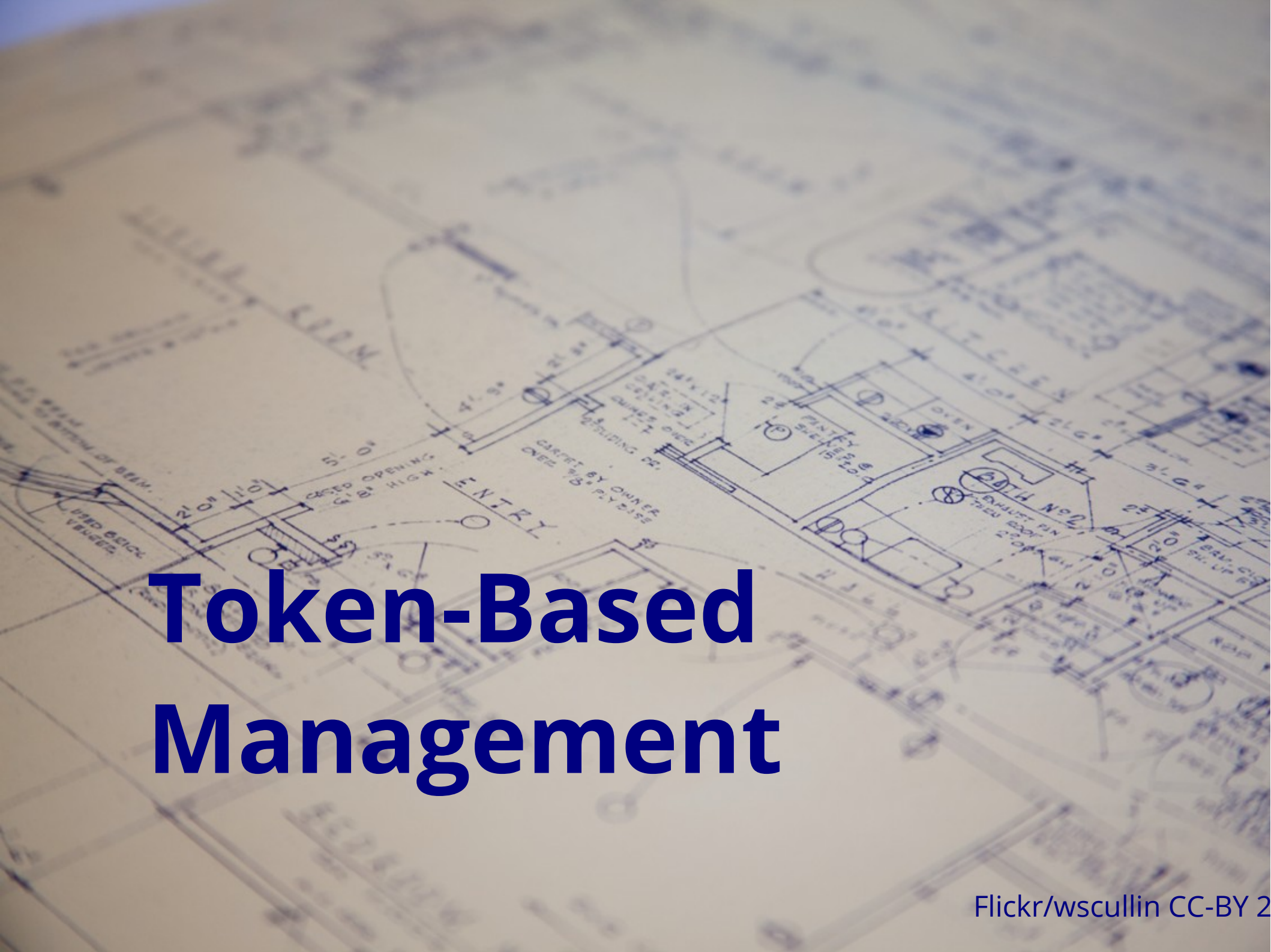
Consent + Regulation

- Controllers need to demonstrate that consent has been sought
- And that the mechanism for doing so was appropriate
- Consent is a **compliance problem**

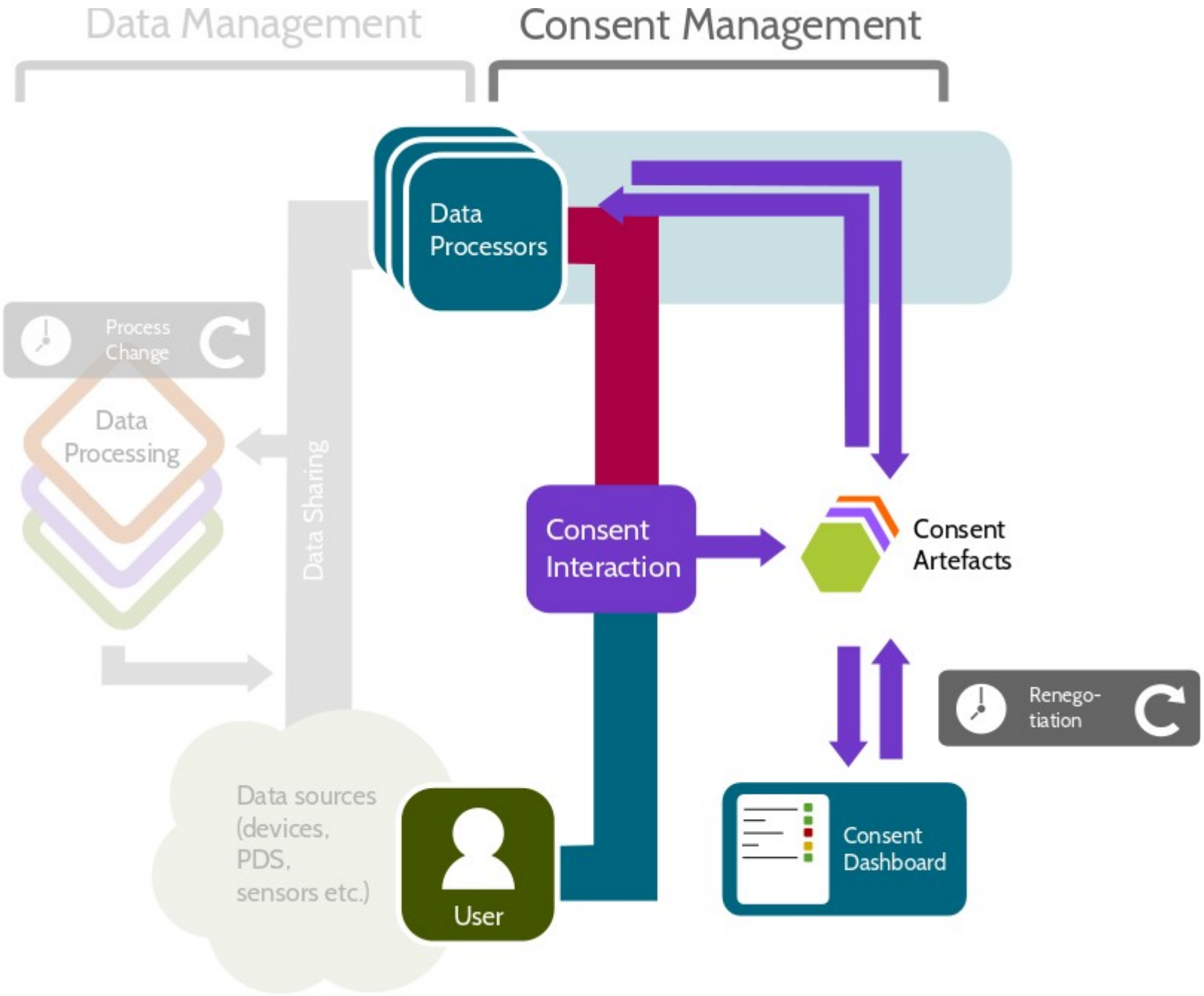
(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[1] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible

Challenges

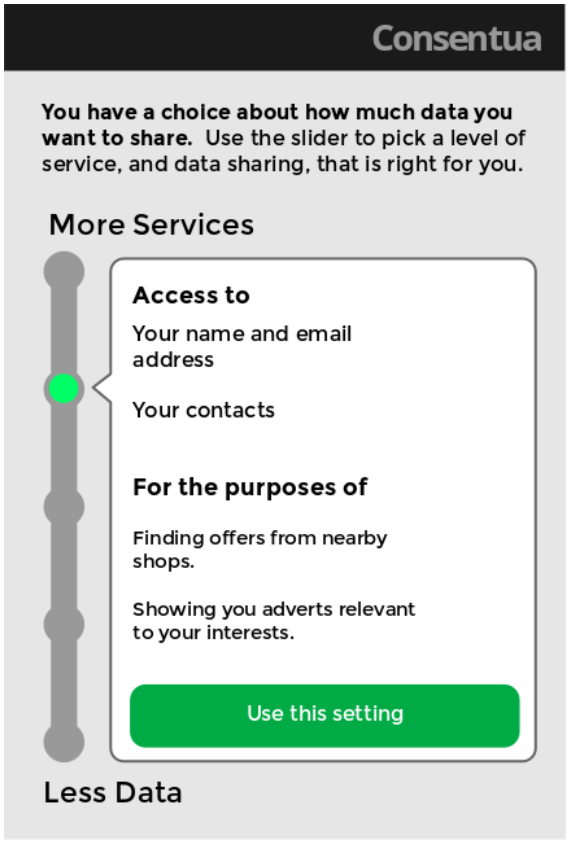
Flickr/m01229 CC-BY-N

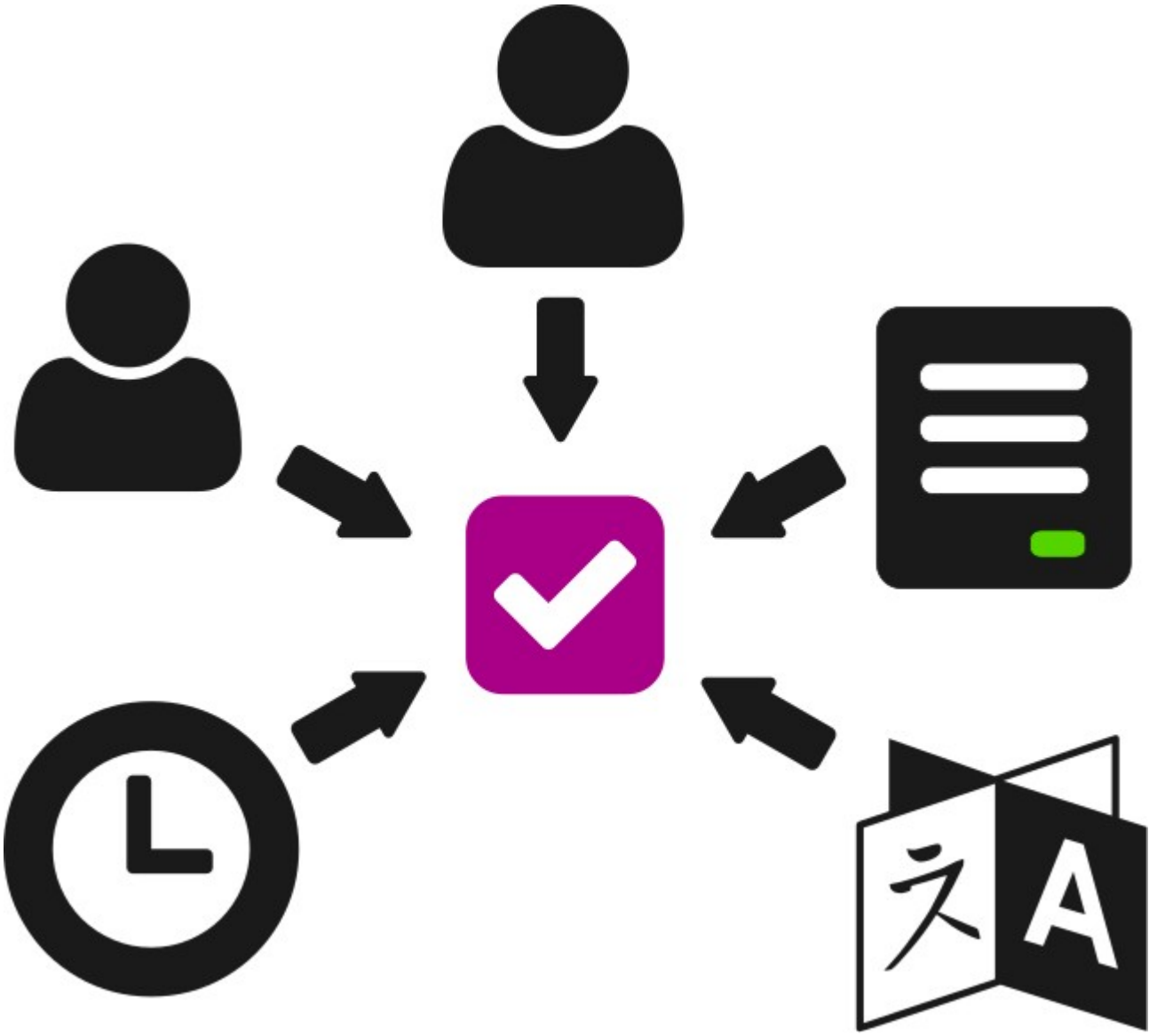


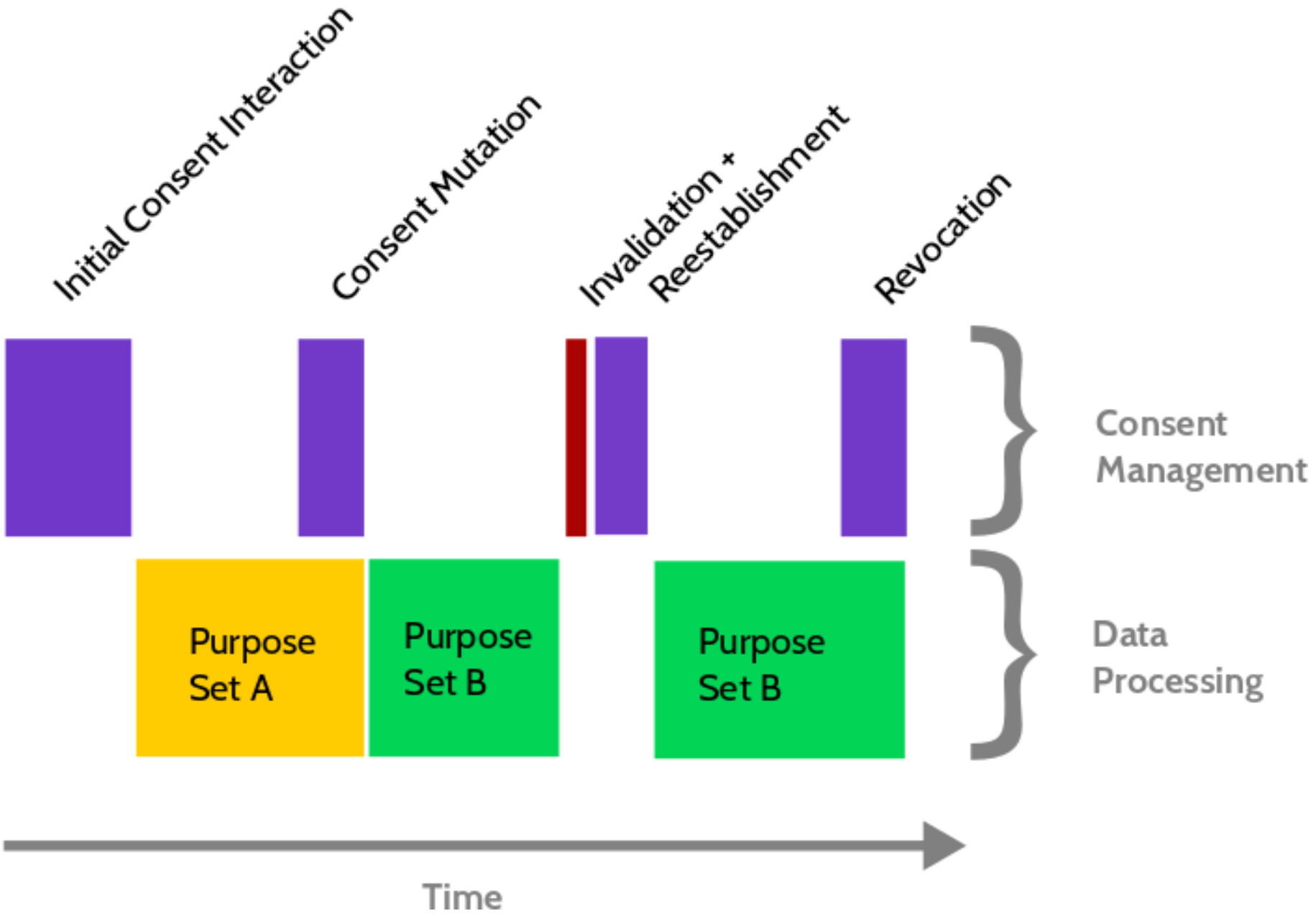
Token-Based Management


Data Management
Consent Management
Data Processors
Process Change
Data Processing
Data Sharing
Consent Interaction
Consent Artefacts
Renego-tiation
Data sources (devices, PDS, sensors etc.)
User
Consent Dashboard

Please send me information about special offers, new products and updates about ACME corp.




A


Initial Consent Interaction
Consent Mutation
Invalidation + Reestablishment
Revocation
Consent Management
Purpose Set A
Purpose Set B
Purpose Set B
Data Processing
Time

Consentua

Your consent record

Search providers by name

Go

Find providers with access to my...

Browsing History

Location

Health Data

Contacts or Social Data

Contact Details

Find providers who use my data to...

Analyse service usage

Deliver targeted advertising

Contact me by email

Consentua

Your consent record

◀ Back

Service Providers with access to your **browsing history**

- The Guardian [www.guardian.com] View ▶
- ACME Mobile App View ▶
- ACME Mobile App View ▶
- ACME Mobile App View ▶
- ACME Mobile App View ▶

Consentua

Your consent record

ACME Mobile App

Read Privacy Policy

Now

Uses your...

For the purposes of...

Modify

History

Updated 16/03/2016

Uses your...

For the purposes of...

Created 12/03/2016

Uses your...

Summary

- Couple data processing to a record of subject consent and, crucially, makes consent decisions mutable
- Provide record of language, interaction and parties for audit purposes
- Detailed reasoning over rich consent artefacts is flexible and responsive to regulatory changes

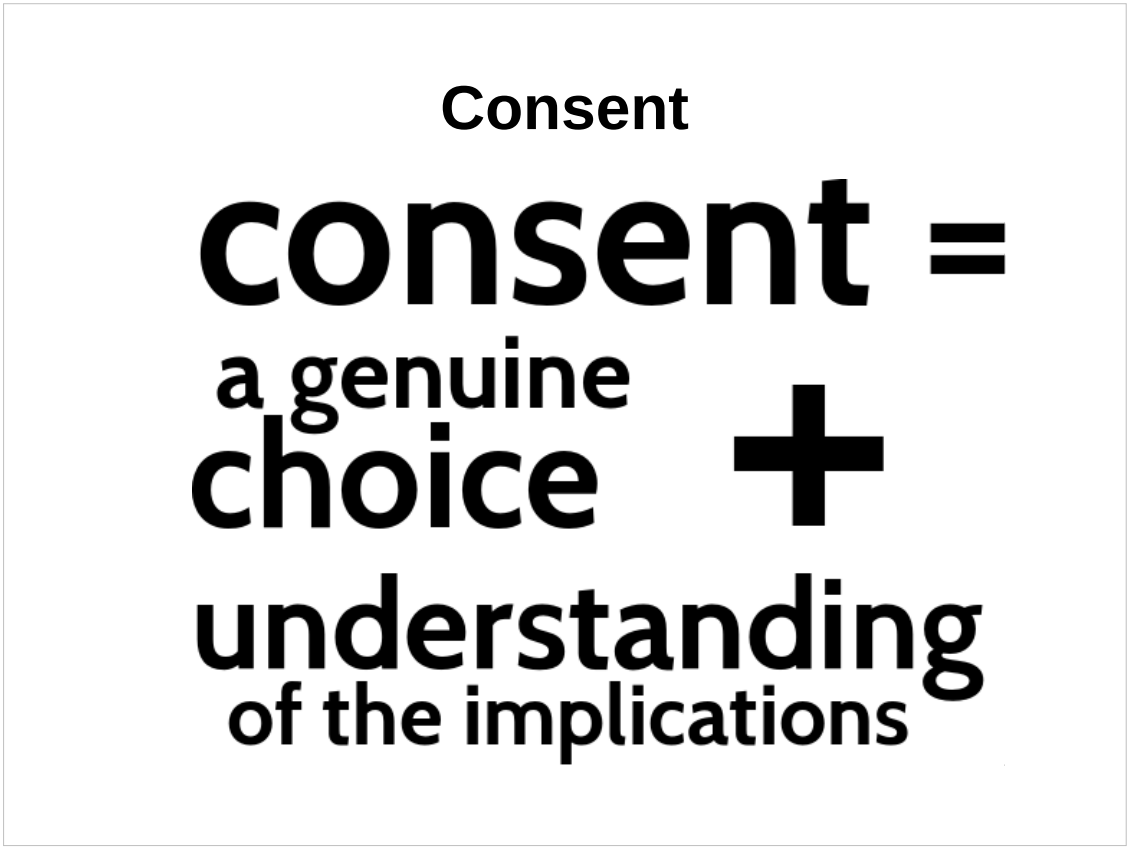
Meaningful Consent in the Digital Economy
meaningfulconsent.org

KnowNow Information
kn-i.com

@richardgomer
r.gomer@soton.ac.uk

My name's Richard gomer, I'm a researcher at the University of Southampton, where I work (among other things) on the meaningful consent in the digital economy project.

I'm here on behalf of a colleague, Chris Cooper, who works for KnowNow information to talk about a model for consent management that stems from the project and which KN are implementing in a platform that they're developing.

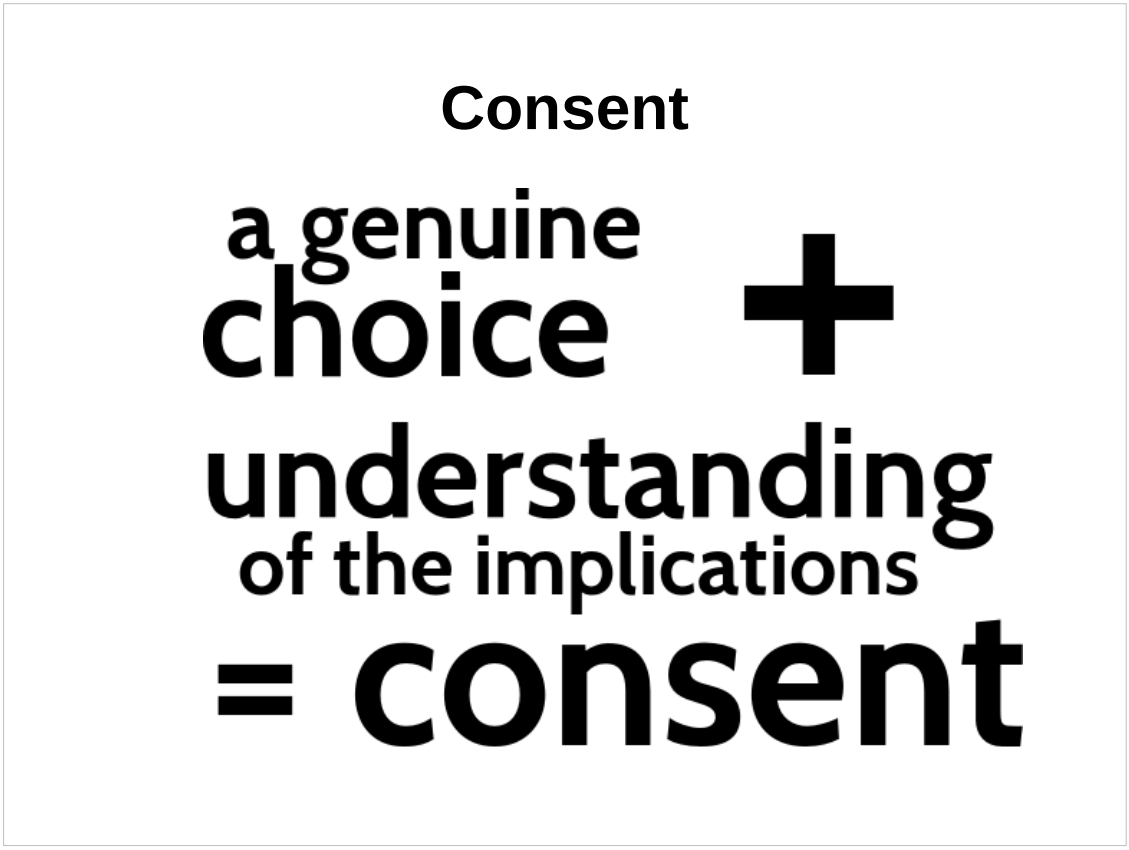


I always like to start with this; to clear up what we mean by consent on the project and to try and dispel some of the baggage around “consent” as a term.

At a basic level, consent in the digital economy consists of giving citizens a genuine choice over the services they engage with, in the presence of sufficient understanding by those citizens of the implications of that choice

There are more nuanced models about how to achieve those two things, but fundamentally that's all that consent is.

Consent may be an explicit signal “I agree” or it may implicit through a voluntary engagement with a service while in possession of the necessary facts



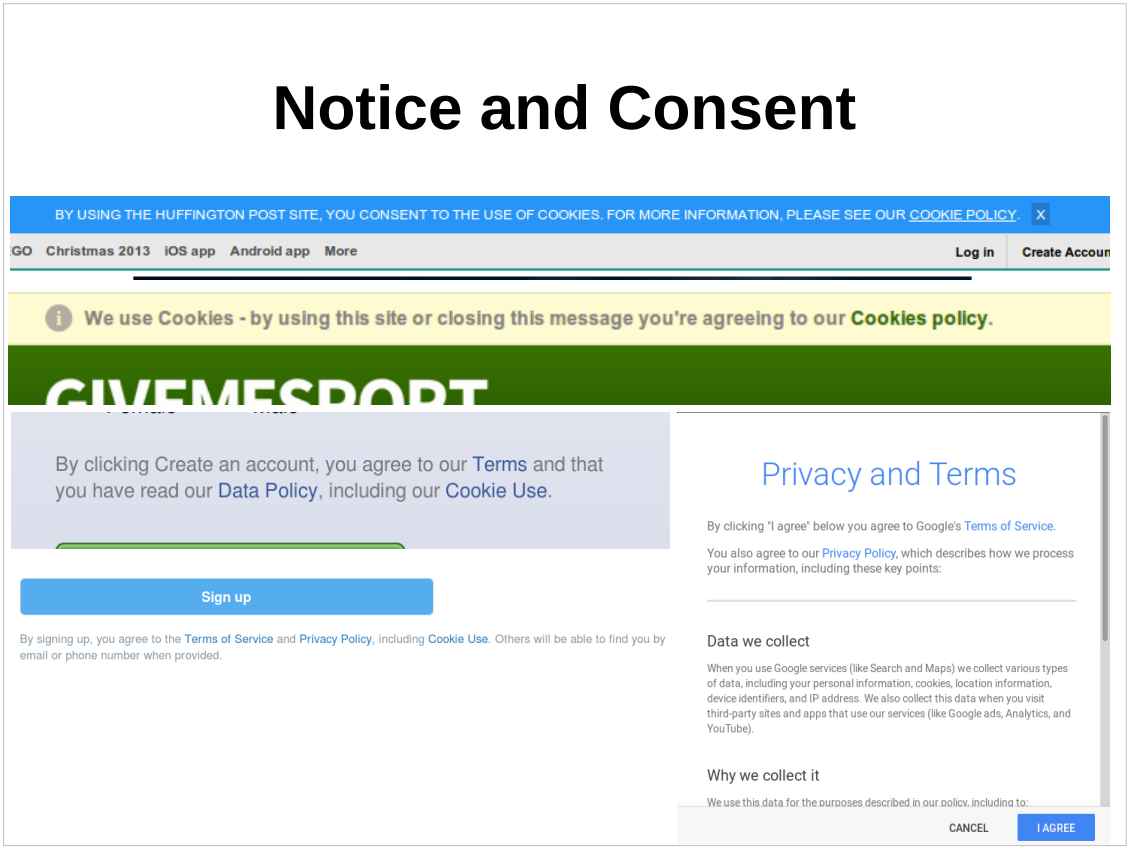
Conversely,if citizens have a genuine choice and understand the implications – that is to say that they know how their data will be processed and what side effects that might have – then they have, in a very intuitive and organic sense, consented.

Choice and understanding of the processes to which citizens are subject are part of what we value in liberal western democracies, and both are part of functional markets where services can be shaped by consumer preference.

Consent is not merely a means to an end in data protection – it is fundamentally *unavoidable* in a digital world that respects these two principles.

Choice and understanding will alleviate the huge trust deficit that exists between digital consumers and the services that they, often reluctantly and with some reservations, engage with.

Notice and Consent



Of course, consent today is typically manifested as annoying boxes on websites; full of dry, incomprehensible information, or something about cookies.

This is one, narrow, class of consent interaction, “notice and consent” it has a number of failings, that aren't really the topic of this talk.

I'd like to encourage you to think beyond these notices and tickboxes, though, and think of consent in a more abstract and imaginative sense!

We can do consent without these; I fact, I think we HAVE to do consent without these if we want to do it well!

Consent + Interaction

- Consent is transactional, it necessarily involves multiple parties
- Consent is an **interaction problem**

Fundamentally, though, consent is transactional, it necessarily involves multiple parties interacting. It is not just a legal problem, it is an **interaction problem**. It requires interaction designers and behavioural science.

Compare the idea of a consent architecture with the Thaler and Sunstein's “choice architecture”

Getting the interaction right is fundamental to realising consent in practice; although exactly how we do that is an open question.

We have some ideas, but, again, not today...

Consent + Regulation

- Controllers need to demonstrate that consent has been sought
- And that the mechanism for doing so was appropriate
- Consent is a **compliance problem**

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[1] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible

Quite pragmatically, from a business perspective, consent is also a regulatory challenge. It has been identified (rightly or wrongly) by policy makers as one mechanism through which digital citizens can be given control over their personal data and, where controllers can't rely on a legiitmate interest justification, it's what they'll be using as the basis for data processing from 2018 onwards.

There are, therefore, compliance questions both in terms of actually doing consent correctly, and showing that you are (and have been) doing consent correctly.

Today I want to talk about how 'token-based' consent platforms can help with citizen empowerment AND compliance.

By consent management, I mean the process of collecting, auditing and reasoning about data subject consent in parallel with data processing operations themselves.

This is a broad topic and one where multiple approaches are possible; but there are a few key challenges that need to be addressed:

As I alluded to previously, auditing collected consent and showing compliance will be a major use case for these systems. In fact, it's probably the number one reason that organisations will make the investment in them.

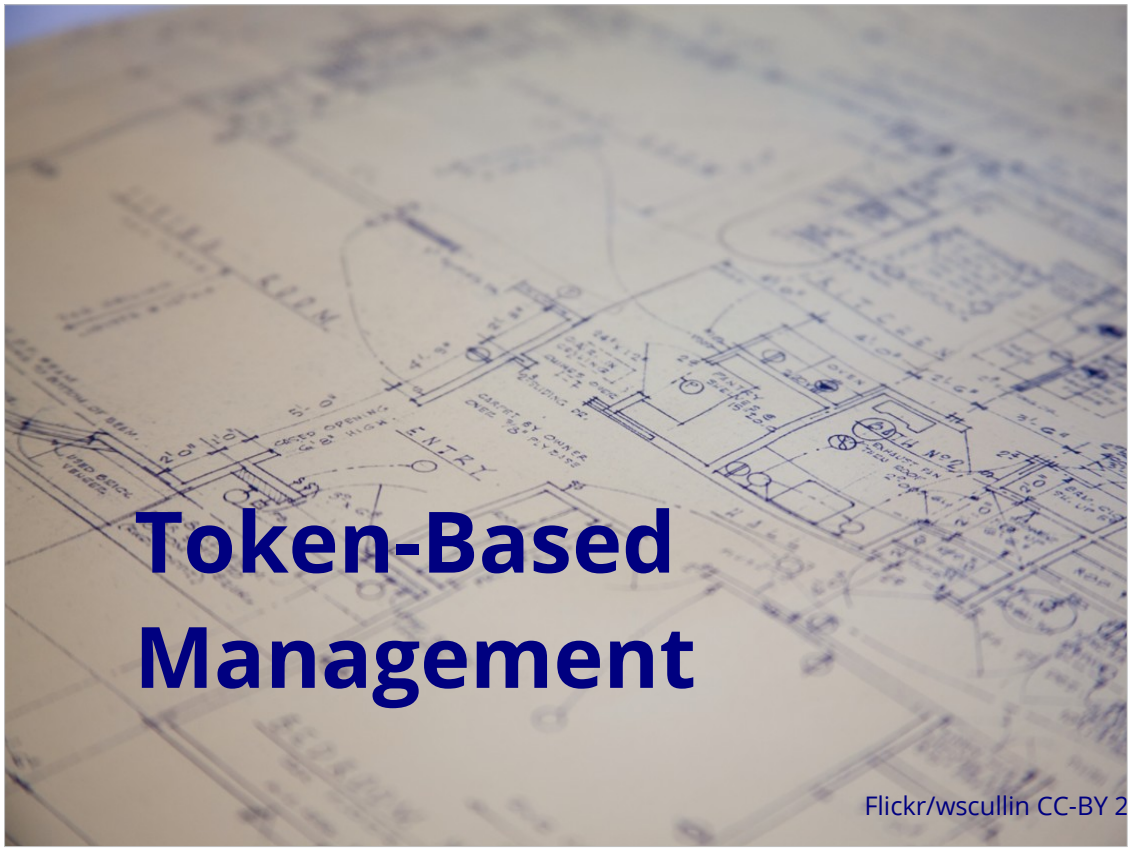
Any platform needs to be flexible and responsive enough to deal with regulatory change;

Not, primarily, huge changes like the GDPR, but constant change in best-practice, opinion and case law. We have to expect that some of the consent interactions that we deploy – some kinds of tickbox, or wording, will be found inadequate later on.

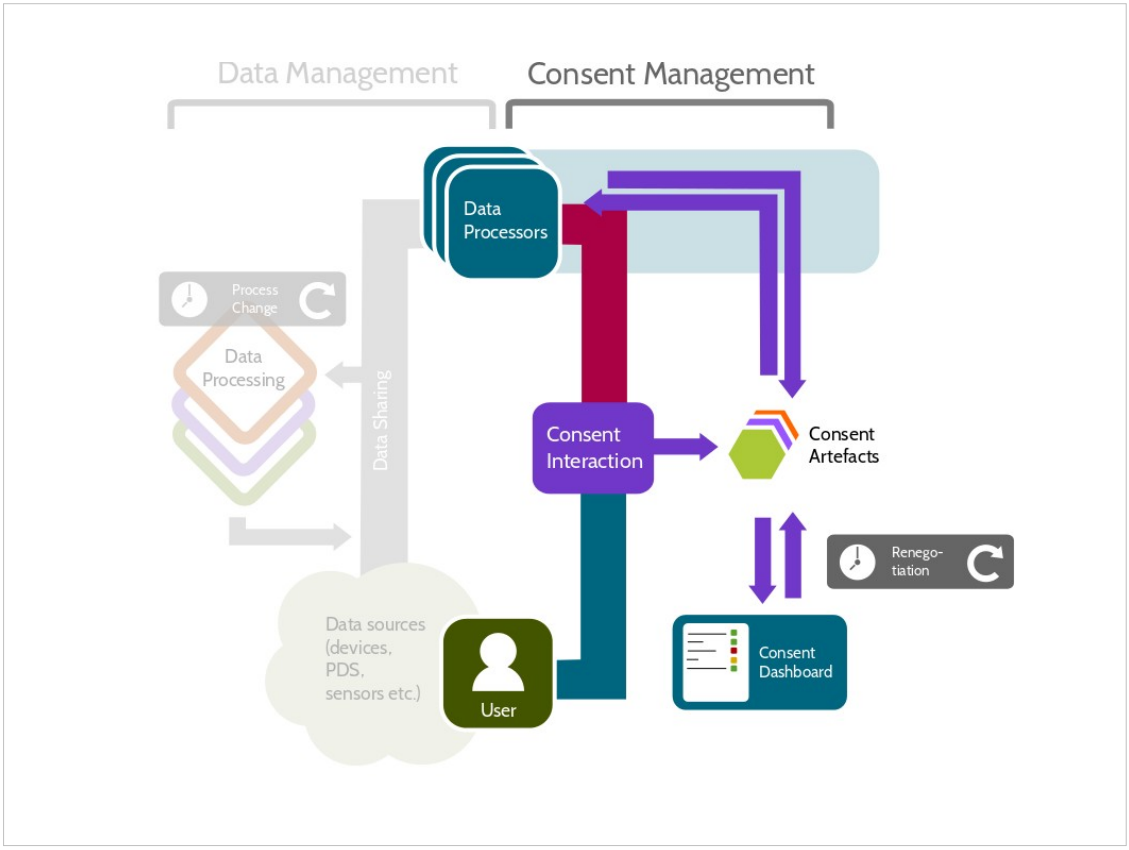
The system itself needs to be flexible enough to change, and crucially businesses need to be able to identify which consent among all of their customers is no longer valid; and, preferably, be able to revisit that.

From a citizen perspective, theses systems have to provide control to data subjects in order to realise the empowering potential that consent is supposed to have.

There is also a compliance angle to this, though – organisations need to make it easy for customers to withdraw consent; and effective, easily accessed, controls will make that possible.



With those challenges in mind , I want to introduce “token-based” consent as an approach to the problem of consent management.

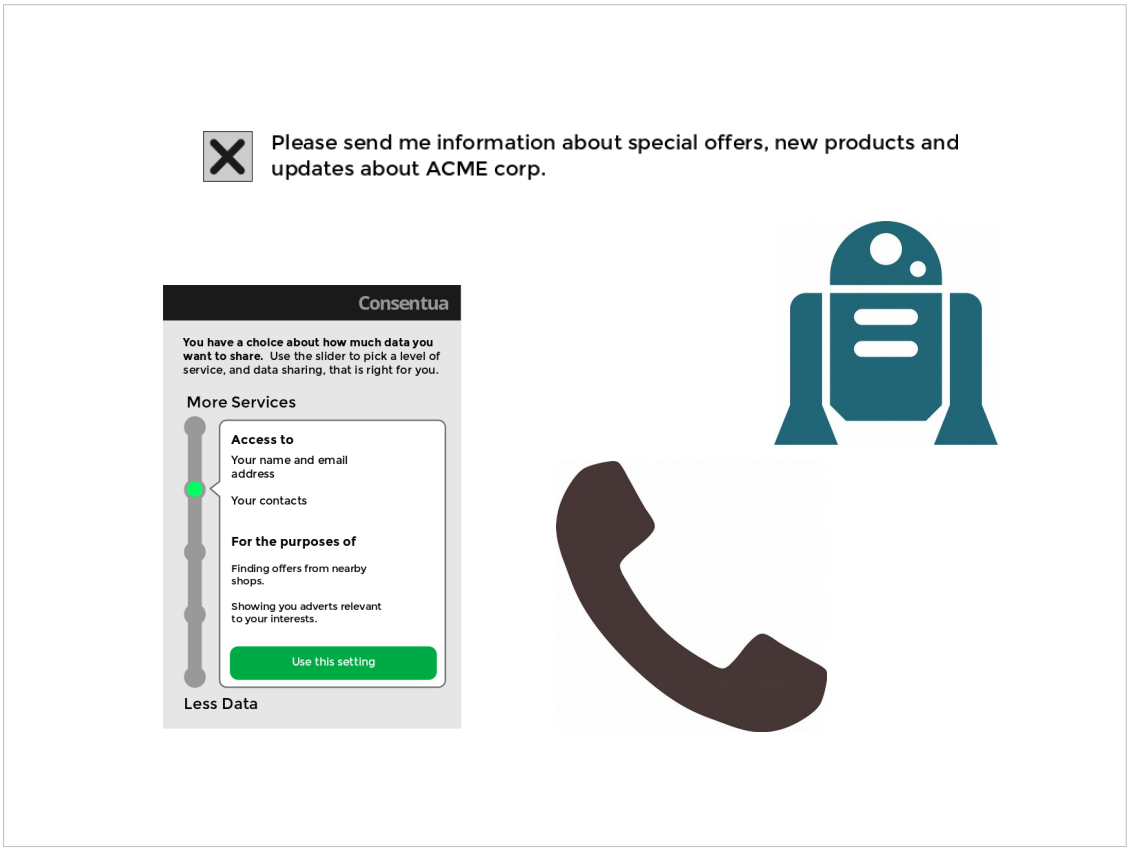


This is a simple diagram of what we mean;

Essentially, consent management is happening in parallel to actual data processing and is realised as two-party agreement between the data controller and the data subject; arrived at through a consent interaction and crucially resulting in some kind of digital artefact; the consent token.

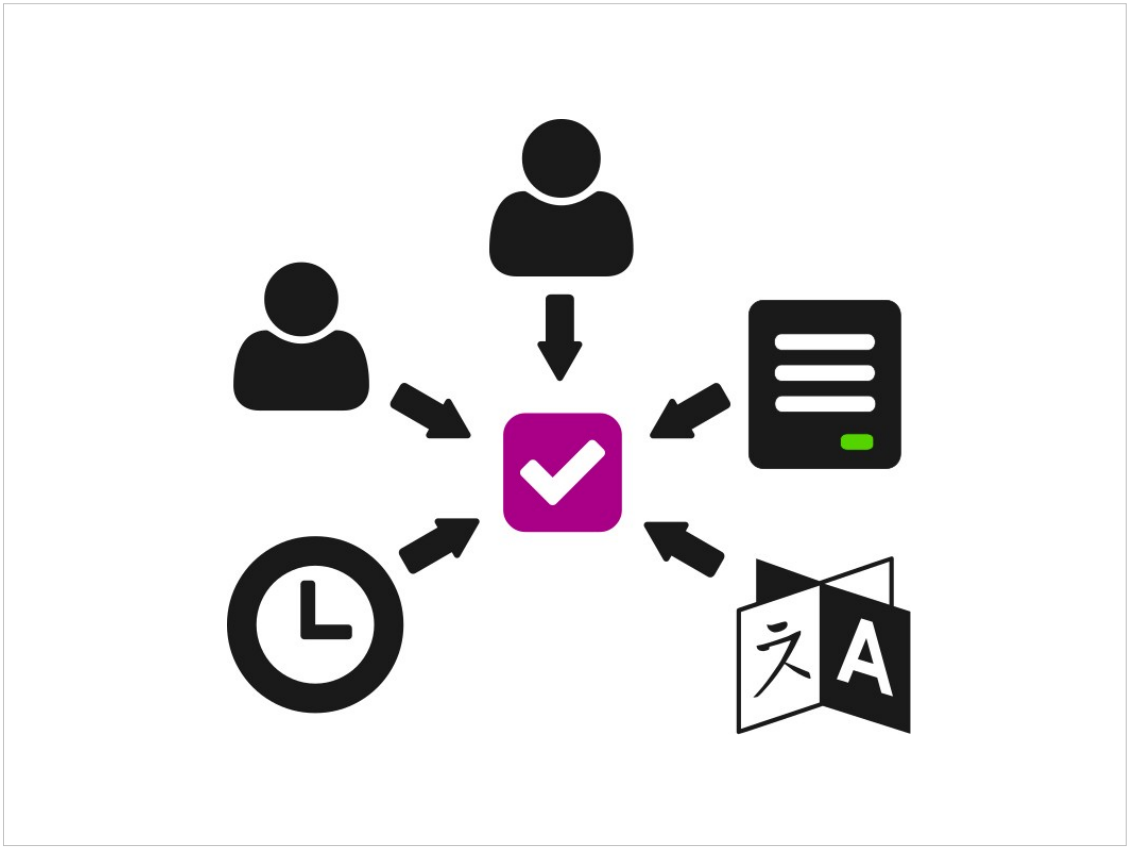
Other groups, such as the Kantara working group, call this a consent receipt.

Both parties have access to this token; allowing them to review the consent that was given. The subject can modify that token, and the controller can check, in real-time, what consent they currently have.



Importantly, this framework is interaction agnostic. The consent interaction that produces the token could be implemented in many ways, depending on the exact requirements of the processing itself (for instance the legal requirements around opt-in and opt-out consent) or based on the medium through which the interaction is being carried out. In some cases, consent will be sought over the phone, on paper, or in automated contexts where there is no screen or conventional input devices.

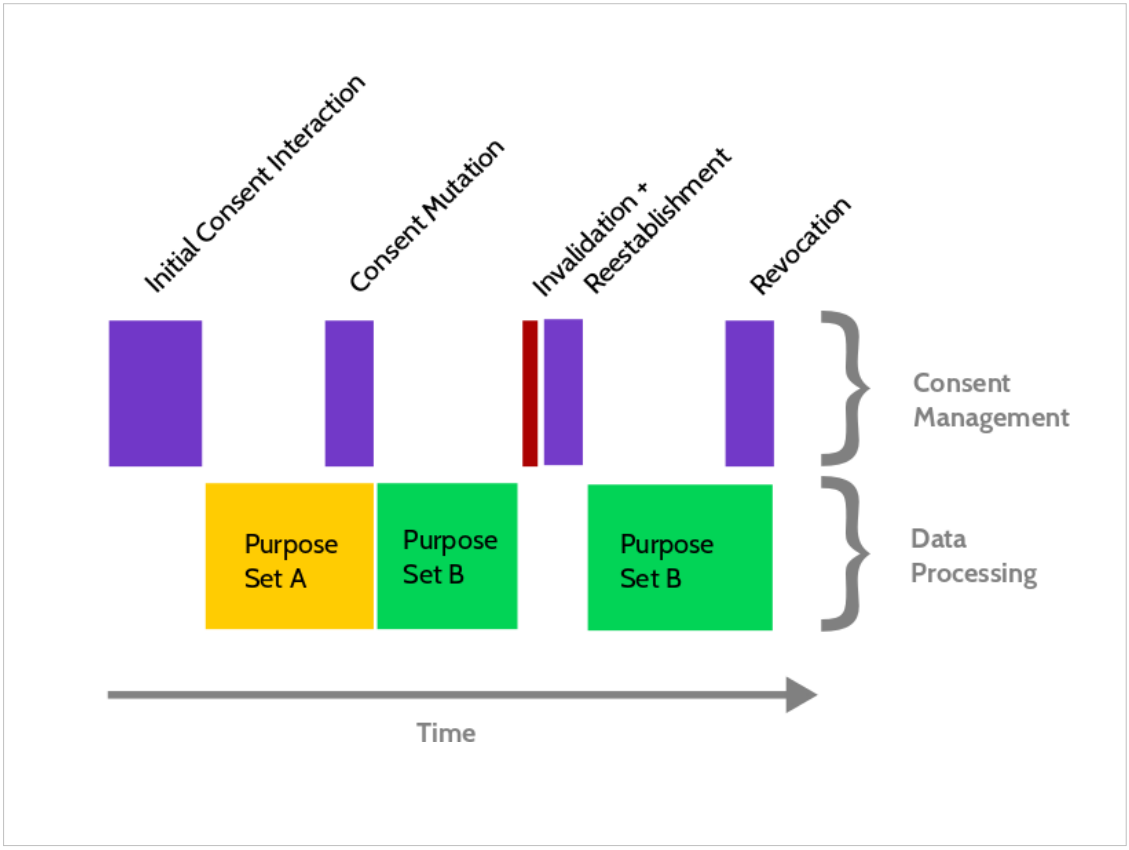
In future, consent may even be given on a user's behalf by a semi-autonomous agent acting for them.



The job of the consent token is to act as a record of WHAT was consented to, and HOW it was consented to.

IT needs to include all the important aspects of the consent interaction, which means at least:

1. Party Ids; who consented to a request by whom.
2. When that consent took place, and any expiry dates etc.
3. The type of interaction that was used, and any important details about that interaction.
4. The concepts and language used in the interaction as may have legal implications later on.

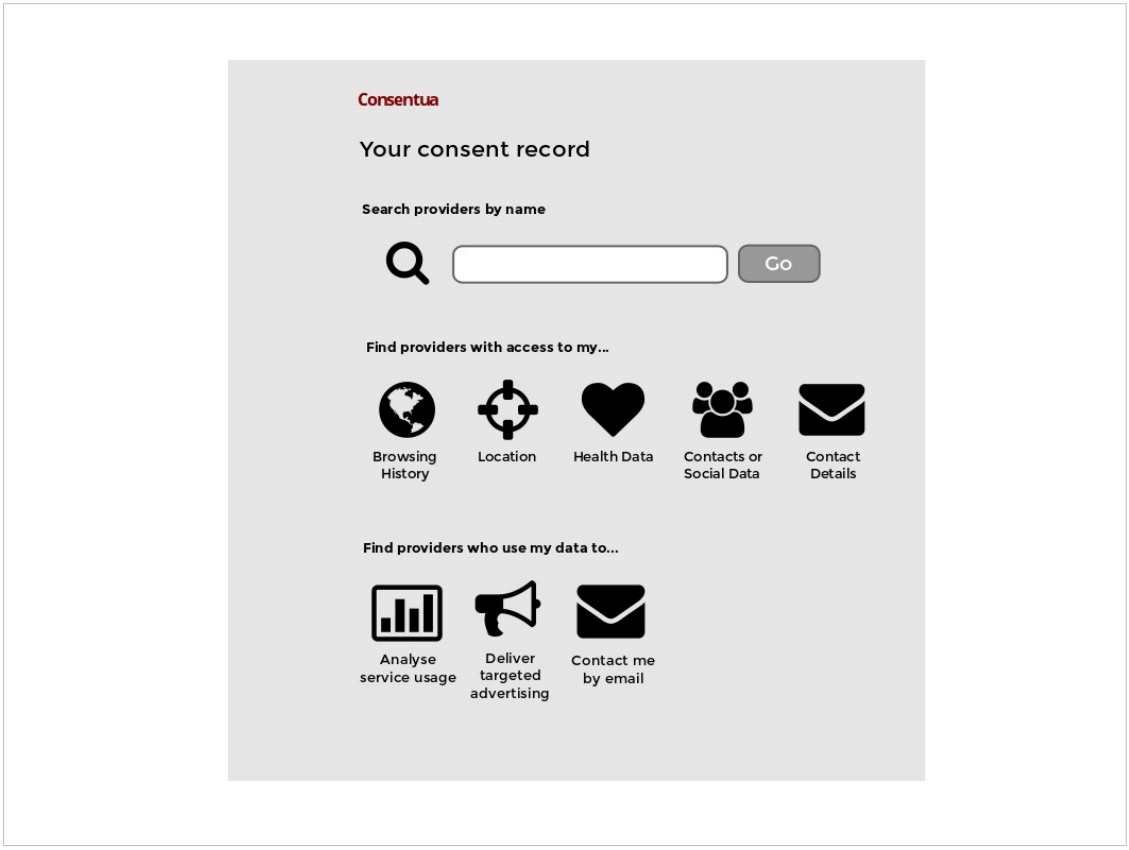


Data processing can then be attached to that consent token, as shown here.

An initial consent interaction generates the token and allows processing by the service provider. Later on, that token is mutated somehow; either by the subject or at the request of the controller, and the purposes for which the data can be processed are altered slightly. Because data processing is contingent on the token, those processes start or stop automatically.

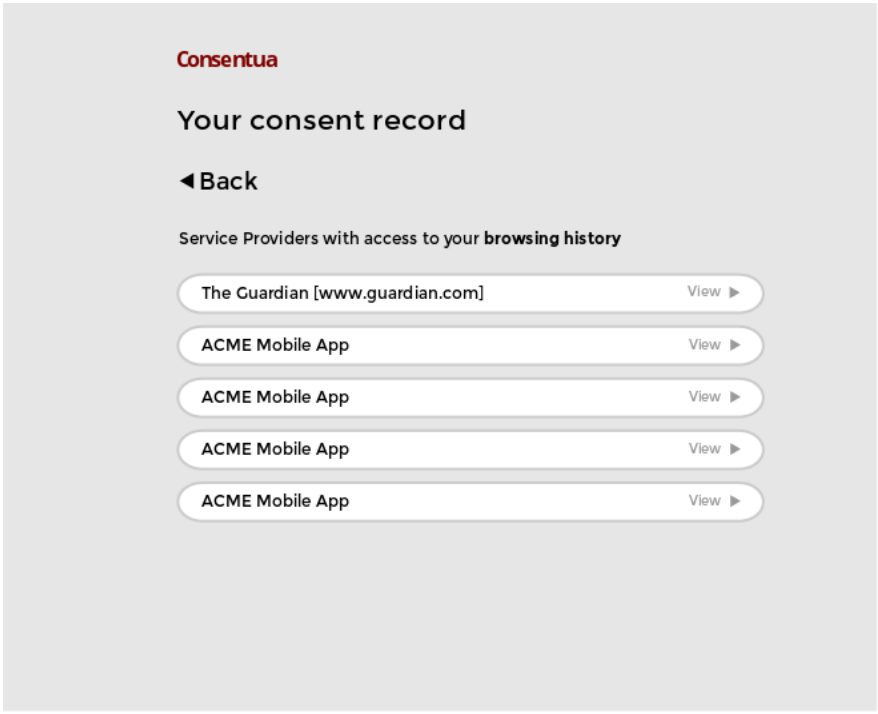
Perhaps later on the initial consent mechanism is determined to be insufficient. All the consent that was sought through that mechanism can be invalidated and – if possible – re-established.

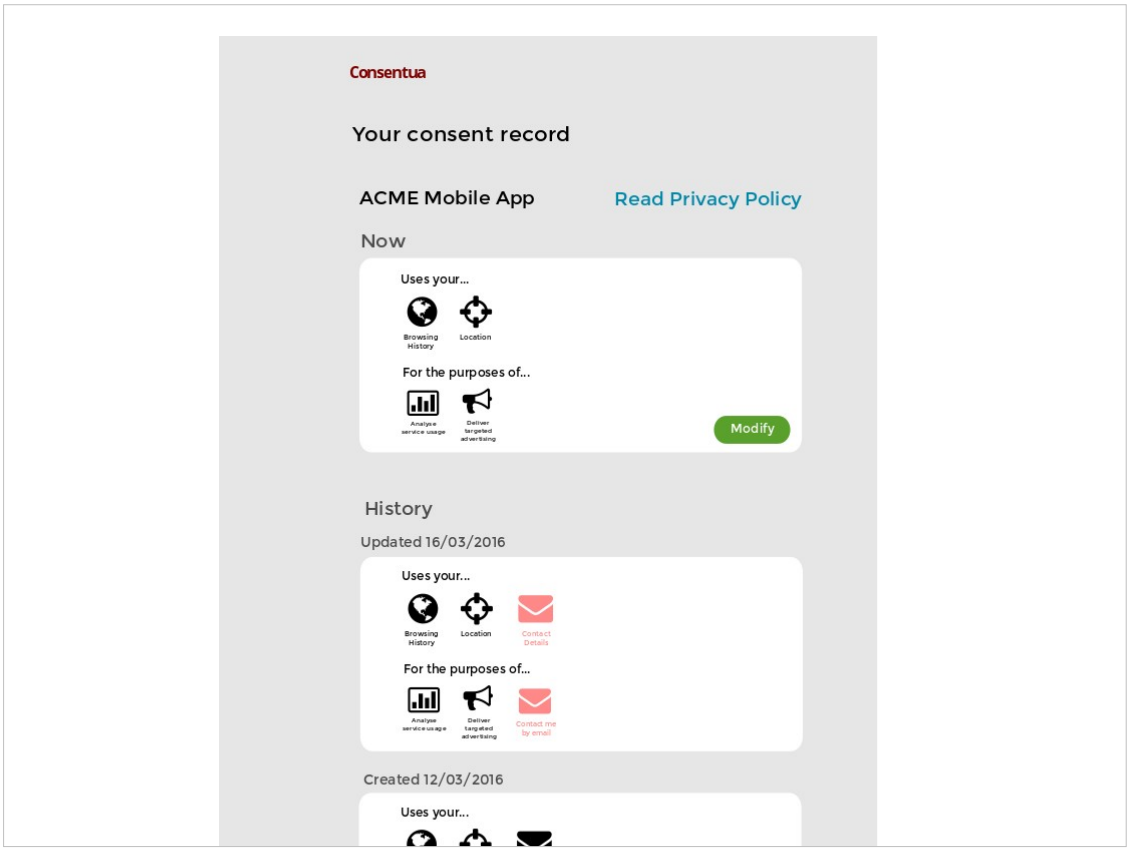
Finally, a data subject can choose to withdraw all consent, or the consent can EXPIRE.



From the data subject's perspective, the consent that they have provided can be interrogated to provide meaningful review features; and mutated to reflect changing attitudes and circumstances.

For instance, you might want to see all the organisations with access to data bout your health, or who have permission to contact you by email. A collection of standardised tokens makes this sort of consent dashboard tractable.


Consentua
Your consent record
◄Back
Service Providers with access to your **browsing history**
The Guardian [www.guardian.com] View ▶
ACME Mobile App View ▶
ACME Mobile App View ▶
ACME Mobile App View ▶
ACME Mobile App View ▶



It also provides the opportunity to view the history of a particular relationship; showing how consent has been altered over time.

Summary

- Couple data processing to a record of subject consent and, crucially, makes consent decisions mutable
- Provide record of language, interaction and parties for audit purposes
- Detailed reasoning over rich consent artefacts is flexible and responsive to regulatory changes

Soo….

That was quick intro to consent management, and the use of token-based management in particular.

Consent management aims to couple data processing with the process of managing consent itself. Consent can then act as a breakpoint in automated systems, at the same time providing direct control to data subjects.

Tokens can record the language, interaction, purposes and parties; allowing consent to be interrogated on an individual or aggregate basis.

Detailed tokens allow audit of the consent management process, and responsiveness to regulatory change.


UNIVERSITY OF
Southampton
Meaningful Consent in the Digital Economy
meaningfulconsent.org
kn-i knownow
KnowNow Information
kn-i.com
@richardgomer
r.gomer@soton.ac.uk
Research Councils UK
Digital Economy
Transforming Business and Society

Thanks!