WHITEPAPER

UNDERSTANDING DIGITAL CONSENT

A COMPREHENSIVE GUIDE TO DIGITAL CONSENT IN THE PERSONAL DATA ECONOMY

MEF
MOBILE ECOSYSTEM FORUM

MEF
GLOBAL CONSUMER TRUST INITIATIVE

Introduction

Consent is at the frontline of the drive to create new standards of digital privacy...

Consent has always been at the heart of any property contract between people. Firstly, a person agrees that another can use his/her property. Then they reach agreement about what the recipient can do with it.

In the digital economy, consent is much more complex.

Because data is so valuable, some companies ask for more data than they need. They want to hold it 'just in case'. After all, storage is cheap: deleting data costs more than keeping it. They also share it with third parties.

And the law hasn't really stopped them. Therefore data has become an asset class and this has led to uncertainty and, occasionally, malpractice. However, customers are waking up to this. They are starting to resist the rampant data gathering. They want clarity on who holds their data and why. Of course, one answer to this is to restrict data sharing altogether.

But that's not a realistic solution. Why? Because people get better products and services when they share information.

So the data privacy problem does not arise from companies asking for data itself. It arises from abuses of this process. This is why consent matters to everyone.

When there is genuine consent:

- **Businesses can build effective goods and services targeted to individuals**
- **Consumers can assign high quality data to companies they trust**

This makes business sense. There's a pay-off when consumers trust more.

"The problem does not arise from companies asking for data itself. It arises from abuses of this process. This is why consent matters to everyone."

A 2017 consumer survey by the Mobile Ecosystem Forum revealed 32 per cent of smartphone users would use a trusted app/service more often than they would others.

It also makes legal sense. In some places higher standards of consent will soon become law. For example, in 2018, the General Data Protection Regulation (GDPR) will compel companies engaging with EU to follow new guidelines on consent.

Companies in other regions may face less regulation. But the same basic principles apply.

Happily, proof of consent is probably one of the easier aspects of data policy to get right.

For example, many businesses would find it a challenge to build a new system for storing and cataloguing every data transaction. Compared to that, revising the presentation of consent forms – and storing consent receipts – is more straightforward.

And once such a system is in place, the enterprise will a comprehensive record of customer consent data.

Ultimately, 'good' consent is the first lever for making data flow freely and safely. This is the key to healthy digital commerce and excellent services.

In this document, we will look at the evolution of digital consent, good practice, law and the companies pushing new ideas and models.

This paper was developed as part of MEF's Global Consumer Trust Initiative, with contributions from its international working group made up of industry stakeholders to gather the information and insight.

"Ultimately, 'good' consent is the first lever for making data flow freely and safely. This is the key to healthy digital commerce and excellent services."

Contents

What consent means: history and definitions

Consent has had a legal meaning for over 100 years. Now, the digital economy demands new definitions...

"Some organisations assume a tick of one box effectively gives them access to an individual's address, browsing habits, bank account number and more."

1. A short history of consent

As a legal idea, consent is little over a century old. It was born in 1908, when a New York court heard the case of Mary Schloendorff. She had been admitted to hospital for a stomach disorder.

The doctors diagnosed a tumour and suggested surgery, which she declined. They went ahead anyway. But later, Schloendorff developed gangrene and had her fingers amputated.

She filed a lawsuit and won (though the judge found the doctors and not the hospital at fault). The judge said: "Every human being of adult years and sound mind has a right to determine what shall be done with his own body; and a surgeon who performs an operation without his patient's consent commits an assault for which he is liable in damages."

109 years later, the issue of consent is a hot topic again – thanks to the migration from analogue to digital. You merely have to amend the judge's comments as follows to see how:

"Every individual has a right to determine what shall be done with his own data."

2. The challenge of consent in a digital economy

The new digital economy depends on the flow of data to create attractive, targeted products.

So some firms grab what they can, while their lawyers write 20,000 word privacy notices that mostly go unread. These organisations assume a tick of one box effectively gives them access to an individual's address, browsing habits, bank account number and more.

The balance has been tipped massively in favour of digital vendors.

New ideas began to emerge around 2008. The digital thinker Doc Searls encapsulated them in his book The Intention Economy.

He argued that in traditional negotiations, two parties come to an agreement that suits them both. But when one entity serves millions of customers, this arrangement cannot work. The net result is 'adhesion' contracts running to millions of words that load all the power in favour of the enterprise.

Searls argued for a new model. Here, customers take control of their data and release it only to trusted third parties. He called this process 'vendor relationship management' and named the wider idea the 'intention economy'.

He stated that customers should be able to say: "This is my personal data place, where we store personal data that is useful to us in market interactions and also our preferences and policies, terms and services. For example, 'give me back my data when I'm done with it. Here are the things you can look at, here are the things you can't.'"

Searls was ahead of his time. He paved the way for the rise of a new breed of startups (personal information management companies – PIMs - see section) that are trying to create a personal data economy.

He also anticipated the changing attitude of regulators, not least in Europe when GDPR will impose new laws on data privacy (see section).

3. Multiple types of consent

There is more than one way to give consent. This partly explains why the topic has become complex – especially in the digital realm.

As a general rule most services display a consent box with a notification that says what the person is signing up to. The form will offer either active consent (with a tick box) or some kind of implied permission (wherein the act of using the service grants consent).

Here is a more detailed description of these different types of consent.

Informed consent

All consent should be informed. Broadly this means that a person must understand what they are signing up to. This compels the supplier to use clear and understandable language. It also means that, in most cases, children and people affected by mental illness are not legally competent to give consent.

"All consent should be informed. Broadly this means that a person must understand what they are signing up to."

"There is more than one way to give consent. This partly explains why the topic has become complex – especially in the digital realm."

If we accept that an individual is properly informed, then comes the question of how they give their consent. This depends on various factors such as the medium, the topic and the level of risk.

These factors will determine whether informed consent is implied, passive or explicit.

Implied consent
Here, participation with a service is in itself proof of consent. For example, an individual might sign up for an online competition. He gives his email and accepts he will be contacted. But he does not sign anything to say explicitly "I agree to the processing of my personal data". This is implicit in his participation.

Explicit, express or active consent
With explicit consent, a participant must give clear and documentable consent to the terms of the agreement. This will usually take the form of ticking a box or signing a form that clearly describes the data to be shared. In extremely sensitive instances (personal medical data collection, say), the user might even need to sign a document or send an email.

Opt-out consent
Here, if the user does not clearly decline consent, permission is granted. Most readers will be familiar with sites that share personal information unless a pre-ticked box is unticked.

Exceptions
There are scenarios is which an organisation can collect personal information without consent. Examples include the hospital treating a medical emergency or governments dealing with national crises.

Regulation

1. EU: General Data Protection Regulation (GDPR)

From May 2018, companies active in the European Economic Area (EEA) and multinationals offering services to EEA residents will be bound by the General Data Protection Regulation.

GDPR will impose new restrictions on how companies collect, store and share personal data. And consent is one of the six legal bases a company can use to hold an individual's information. The six are:

- **Consent**
- **Contracts**
- **Legal compliance (with another law)**
- **Protecting the vital interests of a person**
- **Public interest**
- **Legitimate interest**

GDPR defines consent as follows: 'Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'.

The law changes consent practice as follows:

More transparency

Enterprises can't just say 'click here to read our Privacy Policy'. Now, they have to use plain English to explain why they are collecting personal data at the point they are collecting it.

Then they must explain how they plan to use it. And if they plan to share it with third parties (even Google Analytics for example) they will need to get explicit consent for that too.

No more implied consent

It used to be that signing up for a service was, in itself, enough to imply consent. No longer. The regulation states clearly that "silence, pre-ticked boxes or inactivity should not constitute consent".

No more bundled consent

Consent requests must be separate from other terms and conditions. Consent should not be a pre-condition of signing up to a service unless necessary for that service (see box on 'GDPR and mobile apps').

GDPR and mobile apps

Apps collect private data so, self-evidently, GDPR will affect app developers. In fact, it may provide unique challenges.

For example, the GDPR states that suppliers should outline every kind of data they wish to collect. And they cannot decline access to a service just because a person declines to agree to one of the requests.

But what if an app cannot function without certain data? A ride sharing app, for example, needs access to GPS. It can't work without it. So does it have to ask for consent? Can it decline access to the service without agreement? These questions may have to be resolved by law (using the 'legitimate business' legal base mentioned above).

Another issue concerns app developers outside of Europe. People download apps from global stores like Google Play. These stores comprise apps from all over the world. Can global developers observe the standards demanded by EU regulators? It's possible tools and middleware companies will make their assets 'GDPR ready', which will help. But this remains a serious challenge.

Better access to consent data

The GDPR places emphasis on a users' right to access her own personal data. She must be able to request at any time the data she gave and know what an organisation plans to do with it. That means enterprises must keep records of what individuals consented to. This should include what they were told, and when and how they consented.

Higher standards of consent in special categories

When personal data is "particularly sensitive" the law demands "explicit" consent. Such data includes racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetics, biometrics, health, sex life or sexual orientation. If these details are needed, a user should respond actively to a question, orally or in writing. Clearly, this is very different from the generally accepted definition of 'explicit' consent, which merely involves some kind of tick box or similar.

Children can't consent

Controllers must obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16.

Exceptions

The GDPR states that there are six legal bases for storing data. Consent is used when the others are not applicable. These other legal 'exceptions' include employment contracts and some healthcare agreements (few people would insist on explicit consent when they face a life or death operation).

The exact terms are explained in Article 6(1) of the GDPR as follows:

The processing of personal data is lawful when:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

(c) processing is necessary for compliance with a legal obligation to which the controller is subject

(d) processing is necessary in order to protect the vital interests of the data subject

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. EU ePrivacy

The EU ePrivacy directive governs how digital companies track individuals. It has become known as 'the cookie law'. It is a 'directive' (first drafted to 2002 and revised in 2009). As a directive, it is left to EU members to interpret it.

But in 2016 came a proposal text to make it regulation – and therefore binding across the EU.

The key aim of the new proposal is to simplify the rules regarding cookies. One change will dictate that access to a website should not be conditional on accepting the use of tracking cookies, for example.

The regulation also recommends that browsers play a greater role in managing consents. Users could install extensions that communicate their preferences to the sites they visit.

3. The US/EU Privacy Shield

In July 2016, new rules around the sharing of European's personal data by US companies came into force. The Privacy Shield agreement aims to provide EU consumers with information on what data is moved to US servers and how they can make complaints if they feel rules have been broken.

Privacy Shield replaces the previous Safe Harbor framework, which relied on organisations to merely state that they complied with EU rules. The new system has a dedicated US ombudsman to handle complaints. Companies signing up to the Shield must abide by guidelines such as deleting personal data when it is no longer necessary.

4. Brazil: Data Protection Bill

There is no general data protection law in Brazil. However, the Brazilian Congress is considering a new bill governing the use of personal information. It builds on previous legislation such as the Brazilian Civil Rights Framework for the Internet (Internet Act).

The latter says data controllers must provide data subjects with clear and complete information regarding the obtaining, use, storage, processing and protection of their personal data.

They must also obtain express separate consent to carry out any data processing operations. The new Bill of Data Protection Act will go further. It may compel enterprises to appoint a Chief Data Protection Officer, for example.

5. South Africa: PoPI: Protection of Personal Information Act

South Africa passed its own data legislation in 2013, and modelled it on Europe's Data Protection Directive. As such, it aims to ensure local companies process data in line with internationally accepted principles.

The PoPI Act mandates rules around how companies collect, process, store and share personal information. PoPI defines consent to be "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information". At time of writing, only certain sections of POPI had passed into law.

What consent looks like now

The digital economy lacks consistency in how it presents, stores and manages consent forms...

1. Current norms and practices

There is no universal template for 'good' consent models.

So enterprises follow their own instincts. The norm is 'implied consent'. Here, the very fact of using a service – usually granted with a single tick box on a very long 'terms and conditions' form – is enough to grant consent to use a person's data.

In this scenario individuals will have no clear idea of what data has been exchanged. They may have filled in name, address and other details in a form, but they won't know how long this data is to be stored for.

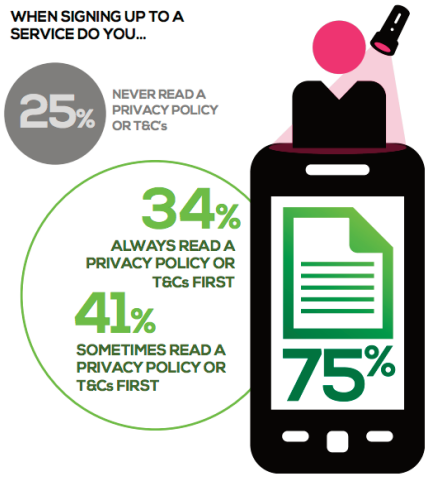
Ultimately, it's difficult for a person to know who has been granted access to his or her private information. Research suggests individuals are becoming concerned about this.

A Mobile Ecosystem Forum study in 2017 found consumers spend more time than most would assume managing their privacy.

- **75 per cent say they always or sometimes read a privacy policy before signing up to a service.**
- **46 per cent say they want to be asked permission whenever their data is collected.**
- **50 per cent want to be asked permission whenever new data is collected or is to be shared differently.**

2. 'Good' consent: design, record keeping and governance

As of 2017, there is clearly no consensus on 'good' consent. But coming legislation and shifting consumer attitudes will change this. That raises the question: what does good consent look like?



source: MEF Consumer Trust Study 2017

In 2017, the UK Information Commissioner's Office set out some ideas in draft guidance. They include:

- ***Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.***
- ***Include the name of your organisation and any third parties, why you want the data, what you will do with it, and the right to withdraw consent at any time.***
- ***You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.***
- ***Wherever possible, give granular options to consent separately to different purposes and different types of processing.***
- ***Keep records to evidence consent – who consented, when, how, and what they were told.***
- ***Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.***
- ***Keep consents under review and refresh them if anything changes.***
- ***Build regular reviews into business processes.***

3. Plain language presentation

PIMS start-up Digi.me has built on these guidelines. It recommends organising consent forms into six plain-language categories and presenting them as follows:

- What data we want
- What we will do with it
- What we will give you back in return for the data
- What data we will keep
- What will we share with third parties and why
- How we give you right to forget/erase/revoke

4. The challenge of consent fatigue

No matter how simple consent forms are, there is a real danger that consumers will view them as an irritation. Most individuals want fast access to services. And they will prioritise this over consent considerations. When presented with a pop-up, they will close it.

This is evident in the response to the "Cookie law" adopted by EU countries in 2011. The regulation has certainly raised awareness of cookies, but it's not clear people understand the choices and consequences. Moreover, consent forms can be especially irritating on mobile, where the form can cover the page and ruin the user experience.

The danger of doing the 'right thing' Case study: Flybe

In the EU zone, the new GDPR legislation mandates that companies must have explicit consent for customer communications. However, there's a very obvious challenge here. If you email your customers to ask for explicit consent, is this email itself a breach of the rules?

In the UK, the airline Flybe found that it can be. It sent 3.3 million emails to customers about updating their marketing preferences, and offered the chance to be "entered into a prize draw" for contributing.

The UK Information Commissioner's Office didn't like this. It fined Flybe £70,000 for breaking the Privacy and Electronic Communication Regulations (PECR) law.

5. Internal processes for managing consent policy

Thanks to new regulation – and rising user concerns around data privacy – organisations will need a more formal internal structure for managing consent.

This means good record keeping. In some cases, large enterprises may need to appoint a dedicated data privacy officer to manage records and consent processes. This individual should have expert knowledge on data protection law and practices.

However, most experts argue that responsibility should extend beyond one individual. Rather, all employees should be made aware of the importance of data protection, and empowered to take some responsibility for it.

6. Storage of consent data

Any organisation that wants to improve its content policy needs to ask: how do we store consent records? This is crucial. With good record keeping, an organisation can easily demonstrate a compliant approach to regulators, answer user requests for information or revoke/transfer records when requested.

Of course, enterprises must consider factors like encryption of the data and which employees have access to it.

Another key consideration is what happens when an enterprise uses cloud-based services to handle consent data (rather than, say, HR).

The business impact of moving from implied to explicit consent
Case study: the RNLI

What happens when an organisation changes from implied consent (a user signs up with a service and implicitly agrees to everything that service does) to explicit consent?

Well, this is what some organisations impacted by GDPR will have to do when the law comes into effect in May 2018.

In the UK, the Royal National Lifeboat Institution charity (RNLI), decided to anticipate that change by moving to an opt-in-only system of communications.

It pledged that, from 1 January 2017, it would stop contacting individuals by telephone, email or post unless recipients had actively given their consent for this.

The charity expected to lose revenue. It predicted a loss of £36m over five years – equivalent to 19 per cent of its income in 2014.

Though RNLI did lose money, it lost less than expected and slashed costs. It targeted only the 900,000 people it knew were engaged supporters, rather than the 3 million in its database. 382,000 opted in.

So, although the total base is smaller, the charity now spends less on outreach and also receives higher average donations. It its annual summer appeal, the response rate was 32.8 per cent – more than triple the rate in 2015. And the average donation was £8.39, compared to £2.94 a year earlier.

It can be cheaper and more efficient for them to do so. But it does complicate the question of data privacy.

An enterprise should always know which cloud services are accessing its data. It must also be sure that cloud apps meet internal security standards, and that it can erase data when it stops using a given service.

7. Anonymisation/de-identification of data

Any discussion of consent assumes that the data in question is personal and therefore identifiable (in combination with other data). In other words, it relates back to a specific individual.

So, obviously, consent is not required for data that is anonymous. For example, a retailer might track the way shoppers move around its store (or website). It might do this to make decisions about where to place tills or 'buy' buttons.

This data would not be assigned to any named individual, so it would fall outside most regulation (and good consent practice).

It's also possible to de-identify information by removing all personal data from the records.

However, this process can be compromised. For example, in 2006 AOL anonymised 20m search queries made by 650,000 users. It replaced names and IP addresses with unique identifier numbers. But hackers compared this data with other sets to reveal identifiable individuals.

GDPR says consent is "not required when a person is not considered identifiable." But as we have seen, de-identifying data is not straightforward.

Still, some regulators are trying to tackle this. In Brazil's Data Privacy Bill, there's a provision stopping companies linking anonymous data to a national ID number, for example.

"It's possible to de-identify information by removing all personal data from the records. However, this process can be compromised."

New consent models, trials and technologies

A collection of innovators is working to find creative solutions to the challenge of digital consent...

"A number of companies can streamline the gathering of consent, making it easier to manage and share profiles."

1. Technological solutions

Consent specialists
If we accept that informed consent is now a critical issue, a good question for enterprises to ask is: can specialists help? Today, there are a number of companies offering technical services around consent. They include ForgeRock, Synergetics, Trunomi, Optanon and others.

These companies can streamline the gathering of consent, make it easier to manage and share profiles. Some offer a kind of 'Verified Consent' or 'Consent as a Service' product, which meets the standards set by regulators (see section on GDPR) around transparency, control and so on.

For example, with Trunomi businesses can request, record and capture consent from customers. For the business, Trunomi creates auditable consent 'TruCert' receipts. These receipts are then converted to dynamic data rights, accessible across all businesses systems. For the customer this provides control and transparency over how their personal data is used. This can be the basis of trusted business relationships and personalised services.

ForgeRock is an identity and access management platform that enables an organisation to draw together identity data from multiple application sources and form them into one profile. A consumer can monitor and manage personal data details, marketing preferences, social login consents, and even wearable device data sharing from a single location.

ForgeRock uses the User-Managed Access (UMA) standard (see section), to help other enterprises gain access to an individual's data – but only when the individual grants permission. Thus, an individual can decide to share information for an hour, a day or forever. Equally, he or she can revoke access any time.

2. The Kantara Initiative: User-Managed Access

All sectors need standards. Consent is no different. The Kantara Initiative is an industry consortium focusing on digital identity transformation. It's working on an open standard called User-Managed Access. UMA builds on the popular OAuth standard that's often employed when mobile app users consent to the app's use of a third party API.

UMA gives an individual a single control point for authorising who or what can get access to their personal data, content, and devices, even across many different sources.

Obviously, this capability can help companies meet new regulatory requirements by letting individuals withdraw consent at any time and generally give back more choice and control. Kantara has also released a draft standard for recording consent.

3. The TM Forum privacy management specification

The TM Forum, a non-profit organization, is working on a framework to give enterprises a set of standards for privacy by design.
The Privacy Management TR243 specification lets organisations create a privacy profile, which can be specific to their own policies or use default settings. End users can also modify their own profiles via a privacy dashboard.

Meanwhile an API will give enterprises the ability to create profiles they can securely (and with permission) share with partners and suppliers.

4. PIMS (Personal Information Management Services)

When consent works well, individuals know what they are signing up for and can revoke their permissions at any time. However, in the real world, people might have relationships with dozens of providers. That makes managing consent difficult.

This is a problem a number of start-ups want to solve. PIMS (Personal Information Management Services) offer services that let people organise their own data and share it with trusted third parties on their terms.

Typically, they provide a web portal or mobile app that puts a user's private information in one place and displays a dashboard of permissions. Enterprises can link to these apps with protocols/APIs that access the data and pull out what they need.

Automated consent Case study: The IBM trust project

At IBM's Research lab in Haifa Israel, technologists are working on a Data Policy and Consent Management (DPCM) platform. It gives companies an automated system for designing forms and documenting all the available data on a specific individual.

IBM has piloted the system its own Watson Health Platform, which helps medical organisations find answers to health-based questions from the cloud. This consent system lets businesses formally model the purposes for which they need personal data and the data associated with these purposes.

Examples of PIMS include Atomite, Cozy Cloud, Digi.me and Meeco.

Though the PIMS market is still embryonic, research by MEF in 2017 suggests that many individuals are ready for it. It revealed:

- **67 per cent say the best party to manage data is 'myself'**
- **26 per cent say the best way to give permission is within a single app.**
- **43 per cent said they'd be interested in an app that could show what data is being collected across all of their devices.**

5. The role of mobile operators

PIMS are not the only companies seeking to return control back to individuals. Many mobile operators have begun to assume this role. Clearly, the telcos possess lots of data on their subscribers. And many consider themselves to be good custodians and well trusted. Now, some operators believe they can harness this combination of curation and trust to offer new services. Examples include:

Orange Trust Badge and privacy wall

The 'trust badge' is an SDK app developers can use to give users clear information on which data points are being collected for which purposes. Orange has already used the trust badge in its own apps.

Meanwhile the 'privacy wall' is a browser plug in that lets people block web trackers, aggregate passwords and gather in one place all online form data. It even supplies a an email or mobile number to avoid spam.

Telefónica Aura

Telefonica wants its 350 million customers to be able to store, manage and sell their own data. Its big idea is to gather all the data Telefónica has about a customer and put it in one place. This will give them transparency, and also the ability to share this data with trusted third parties.

The location for this data trove is a digital personal assistant called Aura. It's an AI powered app that also works with Amazon's Echo speaker. Users can query it about Telefonica and also check a simple traffic-light tool to expose how third party internet applications and services propose to use data.

Deutsche Telekom privacy bots

Germany's Deutsche Telekom ran a competition to find concepts that help consumers better understand their data privacy options. It challenged developers to build digital assistants - bots - to track connected services and adapt a person's data privacy settings accordingly.

Consent receipts Case study: Digital Catapult

The UK's Digital Catapult advises its partners to make their personal data collection forms as transparent as possible. And to set an example, it launched its own 'consent receipt' built using the Kantara Initiative's specification (see section).

So now, when anyone has an interaction with Digital Catapult – including visiting the building – they receive an email itemising the terms of this exchange. This is a receipt that tracks consent just as a paper receipt tracks spending.

Digital Catapult built the platform using standards specified by the Kantara Initiative. Its receipts detail the following information:

- The personal information you gave Digital Catapult
- The purpose of collecting your personal information
- How the information is shared
- How the information is stored
- How to revoke or erase the data

CATAPULT Digital

6. The role of social networks

Facebook Design Jam

Facebook says it wants designers, rather than lawyers, to tackle trust issues. It believes people will share their data (which Facebook's business model relies upon) if they feel in control of the process.

To explore this, Facebook has organised a project called Design Jam. Its goal is to challenge developers to create services that enable this self-control through smart design.

7. AI, digital assistants and bots

In recent years, people have become aware of the idea of the digital assistant. This is a broad-based term that describes a machine that can understand human communication (via voice or text) and respond in the same way.

There are two main types of AI assistants. First, there are the personal digital assistants that can act on behalf of a person. These can be physical – such as Amazon Echo. Or they can be virtual: Apple Siri, Google Now, Microsoft Cortana.

In each case they can open an app, send a text message, schedule a meeting and more.
The second type of assistant is the bot that represents a brand. In this scenario, a person might carry out a text conversation with a customer care agent. But the agent will not be a human. It will be an AI.

Needless to say, these digital assistants need to incorporate user consent when they collect and use personal data. This is a challenging idea. However, it might also be a liberating one.

To a degree, this is what the PIMS are trying to achieve (see section). Facebook is also working on the concept. In 2015 it revealed Facebook M, a personal digital assistant that exists inside its Messenger app. M completes tasks and finds information on a user's behalf.

The company's CEO Mark Zuckerberg believes M can go further and become a virtual entity that understands and applies a user's preferences.

8. User consent and the Internet of Things

For all the hype, the Internet of Things (IoT) is still embryonic. But it does raise important questions around consent for four reasons.

More devices

Currently, people generate data from a handful of sources. With the IoT, it could be hundreds.

Financial services Case study: The FIS Consent Manager

The financial services technology firm FIS has 1.4 million subscribers in its marketing database. To comply with GDPR, it is now re-thinking how these recipients give consent. To do that, it is working with consent specialist Trunomi.

The partners are building the 'FIS Consent Manager'. This gives subscribers a single location for their preferences. Here, they can decide what type of email they want to receive and how often they receive updates.

The FIS Consent Manager tracks every interaction and captures all consent preferences. It then generates signed digital certificates called TruCerts. They prove active, opt-in consent has been received in compliance with GDPR. FIS can track any changes to a person's consent status through Trunomi's APIs.

More sensitive data
Take wearable technology. Any wearable that has sensor, microphone or camera embedded is sharing highly personal information. This is potentially far more sensitive data than 'last website visited' for example. The user must understand what is being shared and who with.

More 'passive' users
An IoT device doesn't just track the person who bought it. A connected CCTV camera is a good example. How can it gather consent from every person it tracks?

User interface issues
It's complicated when IoT devices do not have a screen. This makes it difficult for the user to give consent and for the provider to communicate changes to policy and so on.

9. Blockchain and distributed ledgers

Many experts assume the future of the digital economy will see people store their identities with trusted third parties (see 'consent as a service' section). When asked for personal information from a new provider, they will merely ask their ID custodian to supply it.

The challenge for these identity providers is to keep the information safe and immutable. Many believe the blockchain provides the answer. Using a distributed ledger to store a person's many proofs of ID should be safer than locking it in one server.

A number of specialists are building such services. Evernym, for example, describes these systems as 'self-sovereign identity platforms that can give everyone a digital identity they fully own and control: no one can read it, use it, change it, or turn it off without the user's explicit consent.'

Healthcare Case study: Philips Digital HealthSuite

The healthcare sector is changing. People can use wearables to track their vital signs. Machines that used to fill rooms have shrunk to handheld size.

With so much data available in real time, professionals can anticipate problems rather than react to them. They can also see patterns across groups of users to learn more about a condition.

The challenge is to collect this data in a way that is efficient yet ensures a user's privacy. Healthcare giant Philips built its Digital HealthSuite product to do this. The suite links connected monitors to an app. Users can access their data inside the app and decide with whom to share it. This could be a doctor or a relative. In turn, healthcare providers can return the results of hospital tests to a person's HealthSuite profile.

PHILIPS Healthcare

Research, links and further reading

Regulation

EU GDPR: Key changes
http://www.eugdpr.org/key-changes.html

The US/EU Privacy Shield
https://www.privacyshield.gov/Program-Overview

Germany's Stiftung Datenschutz (Foundation for Data Protection)
https://stiftungdatenschutz.org/english/dataportability-en/

Brazil's Data Privacy Bill
https://clientsites.linklaters.com/Clients/dataprotected/Pages/Brazil.aspx
https://mobileecosystemforum.com/2016/08/05/data-regulation-in-brazil-a-beginners-guide/

EU Draft e-Privacy Regulation
http://www.preiskel.com/the-european-commission-proposes-new-rules-on-e-privacy-and-data-protection-for-eu-institutions/
https://qz.com/883232/eu-cookies-and-eprivacy-directive-the-proposed-regulation-moves-cookie-consent-to-the-browser/

South Africa's POPI legislation
http://www.itnewsafrica.com/2017/06/south-africa-the-age-of-popi-and-what-it-means-for-business/

Best practice

The UK Information Commissioner's Office: PDF on GDPR Consent Guidance
https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

The Kantara Initiative Consent Standard
https://kantarainitiative.org/confluence/display/infosharing/Home

Digital Catapult: personal data receipts project
https://www.digitalcatapultcentre.org.uk/project/pd-receipt/

RNLI: moving towards explicit consent
http://magazine.rnli.org/Article/The-biggest-danger-we-face-Its-losing-touch-with-124

Facebook Design Jam
https://www.facebook.com/notes/facebook-and-privacy/design-jam-in-berlin-delivers-new-approach-to-data-transparency-and-control/1326114810771731/

IBM Consent Platform
https://www.research.ibm.com/haifa/projects/imt/consent/index.shtml

White papers, blogs and insights

MEF White Paper – 'Understanding the Personal data Economy' white paper
https://mobileecosystemforum.com/personal-data-economy-whitepaper/

Southampton University: Meaningful Consent in the Digital Economy blog articles
http://blog.meaningfulconsent.org/

Blog articles on consent by identity specialist Trunomi
http://www.trunomi.com/category/consent/

MyData: thoughts on personal data and consent
http://mydata2016.org/2016/08/12/mydata-the-basics/

Consumer Trust Working Group

MEF MOBILE ECOSYSTEM FORUM

ABOUT MEF'S GLOBAL CONSUMER TRUST INITIATIVE

MEF's Global Consumer Trust Initiative was established in 2012 to raise awareness of importance of building trust in mobile products and services. It helps establish industry best practice and provides practical tools built on the consumer's informed consent. The multi-stakeholder Working Group includes privacy, identity and security experts from MNOs, enterprises, app developers, start-ups and technology providers with legal counsel, product and business executives participating in the initiative.

This whitepaper is part of the working group's work on Building Trust in Personal Data which takes a cross-ecosystem approach to accelerate the development of a data-driven economy and driving long-term sustainability through best practice and consumer choice.

FOR FURTHER INFORMATION AND TO GET INVOLVED PLEASE VISIT:

WWW.MOBILEECOSYSTEMFORUM.COM

MEF GLOBAL CONSUMER TRUST INITIATIVE

ABOUT MEF

The Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. We provide our members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe, Middle East, and Latin America.

ACCELERATING YOUR MOBILE OPPORTUNITY

MEF MOBILE ECOSYSTEM FORUM

MOBILE ECOSYSTEM FORUM

@MEF