CtrlShift

Health & Wellbeing Personal Data Sandbox:

Phase 1 Report

October 2021

Authors
Dr Matt Stroud, Director Ctrl-Shift
Liz Brandt, CEO Ctrl-Shift

In collaboration with Which?

Contents.

Executive Summary.

The last decade has seen an explosion in the number of apps and wearable devices that support consumers' wellbeing. The data generated by these services holds the potential to create huge value for consumers but may also threaten their privacy. Overall, we estimate that the opportunity to create value in a market the size of the UK by sharing Health and Wellbeing data is in excess of tens of billions of pounds per year. This value creation is largest for sectors like health, social care and insurance, but extends into a "long-tail" of value opportunities from video gaming to textiles.

The challenge is of fundamental importance. With an increasingly ageing population and evermore expensive but effective medical technology, the cost of "fixing the sick" is rising at an unsustainable rate. In light of this, societies are increasingly looking to health strategies that "keep the well, well". This evolution from the UK 1940's health architecture is critical to making health provision sustainable and mitigate the suffering that ill-health causes.

Yet to "keep the well, well" necessarily relies on non-clinical health data, that is data from consumer devices. Surveys demonstrate that consumers are reticent about sharing their data from health apps and wearable devices. Indeed the whole edifice stands only one "Cambridge Analytica moment" from collapse. Such a collapse would do real harm to consumers, businesses and society. How to prevent such an occurrence, how to build consumer trust and enable wider value creation through the sharing of consumer Health and Wellbeing data is the subject of this report.

The solutions to consumer mistrust in sharing their Health and Wellbeing data are multi-faceted. They encompass issues of governance, standards, technology, consumer fairness, ethics, liability, and consumer privacy communications. As such, no one organisation is well placed to address the full gamut of issues that must be addressed to develop a solution.

This report was initiated by the Consumers' Association "Which?" who commissioned the specialist personal data and service innovation consultancy "Ctrl-Shift" to develop the work. In order to understand the diversity of issues outlined above, we sought the engagement of a wide range of expert partners, who have contributed their insights. We'd like to thank them for their contribution, while highlighting that the authors are solely responsible for the report's conclusions. These organisations were:

Table of Participants	
Which?	Alan Turning Institute
Amazon Web Services	NHSx
Spencer West	Ada Lovelace Institute
BT	Koa Health
Privitar	CeraCare
Microsoft	Streamr
National Institute of Health Research	Centre for Data Ethics and Innovation
Superdrug	The All-Party Parliamentary Group for Longevity

However today, these value opportunities cannot be fully unlocked. 82% of consumers feel that the benefits of wearable Health and Wellbeing devices are outweighed by privacy concerns. Consumers cite those concerns amongst the top 3 reasons for not using such services.

This reticence on the part of consumers is not ideological. Those individuals most concerned about sharing their data are also the ones who are most willing to share it under the right circumstances. At its core consumers' concerns are rooted in mistrust about what will be done with their data. Left unchecked, these concerns are likely to grow, as technological developments will open the possibility of AI leveraging the data to understand how consumers are reacting to stimuli and then acting to influence them in subtle ways, which are not necessarily aligned to consumers' interests.

When consumers trust the brand, have transparency over what their data will be used for and retain control over their data, they say they will be far more willing to adopt Health and Wellbeing services and share the data generated. In addition to the barrier of mistrust, several other barriers are preventing the realisation of the full potential value of Health and Wellbeing data. The complexity of the sharing process and uncertainty that the consumers will get a fair exchange of value for their data, also act as barriers.

A different type of barrier to value creation relates to consumers' ability to share their data with the services that could create the most value for them. Sometimes Health or Wellbeing services make it hard to share data with 3rd party services for competitive reasons, for instance, if they want to offer such services at a later date. A related issue is that innovators who potentially could create services that would offer consumers new value, can't because they are unable to access training data sets upon which to build the machine learning models that are needed to underpin those services.

The net result of today's, mistrusted, high friction ecosystem is that it cannot provide the basis to realise the true scale of value opportunities. Now is the time to address this, with the market size material, but not yet mature.

To address these barriers we need to create a trusted ecosystem, which offers consumers a trusted way to share their data. The design of such an ecosystem needs to address questions of ethics, governance, liability, consumer communications and technology. Fortunately, the answer to many of these questions exist in the market today, although in a fragmented form, which has not been coalesced or matured into a trusted data sharing ecosystem.

We propose a "solution hypothesis" which takes these components of a solution and orchestrates them into a holistic ecosystem. This solution hypothesis, if backed by a critical mass of organisations, can act as a catalyse for the market to repair and build consumer trust when sharing their data and enable the full value of the data to be unlocked.

Our proposal envisages the "solution hypothesis" maturing via three phases. The first phase can be adopted by an existing stand-alone Health or Wellbeing service and focuses on consumer communication. A "trust seal" would demonstrate adherence to a code of conduct and standardised data labelling would explain to consumers what will be done with their data. The first phase seeks to develop clarity for consumers.

The second phase enables a closed ecosystem of organisations to offer consumers a single consent dashboard to control data. The third stage extends this to enable an open, but privacy-preserving ecosystem in which the consumer processes their data within their own private “data space” and then shares privacy-preserving insights with 3rd party organisations. Most of the technology for the latter phases already exists, but the absence of a widely accepted trust seal or standardised data labelling has inhibited its adoption by the market.

The emergence of a consumer centric trust mark to demonstrably ensure consumer fairness is key to breaking this log-jam and enabling the market’s evolution. However, time is short. Today’s ecosystem is something of a Wild West, comprised of both good and bad actors, which consumers struggle to differentiate. The clock is ticking toward a Health and Wellbeing data scandal hitting the headlines; such an event would fracture what little trust exists, with damaging long-term consequences for consumers, businesses and society.

1. Introduction

1. Introduction.

Data generated by consumers about their activities from apps, wearables and other devices can be used to create insights to support their wellbeing and health. The emerging ecosystem, which is growing up around these data flows, appears to be the subject of some reticence by consumers. Understanding these issues and what needs to be done to create a healthy, scalable and trusted ecosystem is the subject of this report.

1.1 Objectives

This report is based upon the collaborative work undertaken by a number of Health and Wellbeing ecosystem participants drawn from the technology, insurance, health provider, retailer, academic, governmental and legal sectors. Together we set out to address three questions:

1. Which value opportunities does user-generated data unlock?
2. What are the barriers to unlocking that value?
3. What solutions could be envisaged to overcome those barriers?

The first of these questions looks at the potential scale of the market underpinned by trusted flows of user-generated data. In answering it we will scope the value to participating companies and the potential benefits to the consumers.

The second question explores whether this potential value can be realised, and if not why not? These barriers represent both a potential consumer harm and commercial loss to the ecosystem as a whole.

The final question explores the potential of the solutions to overcome the barriers. These solutions may require individual actions, collective actions or require public policy interventions.

1.2 Methodology

At the heart of our methodology was the need for a collaborative, cross-ecosystem engagement, to better understand the issues involved. Since there are many interdependent actors in the Health and Wellbeing data sharing ecosystem, the market must incentivise all participants to coordinate their actions to collectively deliver the optimum value to the consumer.

Failure to optimise the value creation can be driven by the actions of one group of firms or by collective actions/inactions across the ecosystem. Further, each type of actor must work within their own technological, commercial and brand constraints. This necessitates a collaborative approach to our questions, to understand these constraints and identify the barriers to value creation. It is only with all the stakeholder's groups collaborating that we can then explore solutions with confidence that they are implementable across the value chain.

In developing the work described in this report, we engaged each of the participants bilaterally and through a series of collective expert meetings to discuss and ideate key issues. Their input has offered numerous insights and has been invaluable in crafting our conclusions. In addition, we undertook open-source research on existing solutions and components of solutions that are already in the market today.

We would like to thank the organisations who have collaborated and contributed their time and insights to the preparation of this report, including: Which?, Amazon Web Services, Spencer West, BT, Privitar, Microsoft, National Institute of Health Research, Superdrug, Alan Turning Institute, NHS-x, Ada Lovelace Institute, Koa Health, CeraCare, Streamr, Centre for Data Ethics and Innovation, and The All-Party Parliamentary Group for Longevity. Their contribution has been invaluable, but the authors are solely responsible for the reports conclusions.

1.3 Report Structure

This report opens by reviewing the subset of the Health and Wellbeing market which is underpinned by user-generated data. We explore its scope, structure and segmentation. We then draw upon open-source data to identify market trends and estimate its commercial scale, before looking further ahead through the lens of future innovations.

Against this backdrop, we then look at the potential value opportunities which could be unlocked by user-generated Health and Wellbeing data. We estimate the scale of these opportunities and consider which groups of market participants are best placed to deliver them.

Before turning to the barriers to realising these value opportunities, we explore the perspectives of each group of ecosystem actors. This is intended to make plain their likely strategic priorities and constraints. This adds further texture to our understanding of the barriers to unlocking the potential value opportunities.

In the next section, we identify and analyse the barriers to the unlocking of the value opportunities. These span consumer control over their data and trust, complexity and perceived fairness of key elements of today's ecosystem.

In the fifth section, we identify a "Solution hypothesis" to overcome the barriers. We start by identifying the potential components of a solution, based on expert workshops, bilateral meetings, open-source research and Ctrl-Shift's previous experience. These components are then analysed against their ability to overcome the barriers to value creation and their maturity, enabling us to propose a phased solution hypothesis.

In the next section we analyse the components in our Solution Hypothesis and make some high-level recommendations for further consideration in the design phase.

Finally, we close with the section, "The Way Forward", in which we outline our approach to the next phase of this work, the "Design" phase.

1.4 Prologue

Over the last 4 decades, national healthcare costs have escalated, driven by the ageing population and increasingly complex and expensive health interventions. At the same time, consumers are increasingly acting on their desire to increase their wellbeing to live healthy lifestyles. Against this backdrop, Health and Wellbeing data has a pivotal role in supporting consumers to maintain their wellbeing and mitigate the rise in healthcare costs.

In the UK between 1950 and 2020, the NHS's budget as a share of GDP has doubled[1]. Such a rate of increase is unsustainable and so population-level health strategy is increasingly focused on "keeping the well, well", rather than only "fixing the ill". Yet today, the majority of data that exists to understand the wellbeing of the "well" is from consumer devices. To fulfil the ambition of keeping the well, well requires the chasm between the consumer and clinical data spheres to be bridged.

Post-Covid, the ability to leverage user-generated wellbeing data to support healthcare has increased in importance. For example, it's estimated that 10% to 20% of COVID-19 victims go on to suffer from "Long-Covid" and so there is a need to monitor and support them in a scalable and sustainable way.

1. Nuffield Trust 2018: https://www.nuffieldtrust.org.uk/news-item/70-years-of-nhs-spending#then-and-now
2. ONS 2021: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/datasets/homeworkingintheuklabourmarket

2. Context & Market Trends

2. Context and Market Trends.
Key Takeaways

In this section, we review the Health and Wellbeing data market, describing its trajectory, scale, scope and the key trends that are shaping it today. We also look at some of the innovations that will accelerate its growth in the future.

- We define Health and Wellbeing data as:

  "Data that consumers generate by using their digital services and devices, outside of a clinical setting, that supports their Health and Wellbeing."

- The UK Health and Wellbeing is already sizable and growing:
  - In 2018 the app market was worth £1.3Bn with 66% of UK adults having downloaded a mobile health app.
  - Between 2017 and 2021 the wearables market grew, with a CAGR of 11%, and smartwatches starting to displace fitness trackers.
  - Further growth is predicted with a new generation of sensors coming to market over the next decade measuring biometric, emotional and brain states, unlocking powerful new use cases.
- Today there appears to be a limit on the value created from Health and Wellbeing data:
  - 30% of insurance companies globally have used wearable data as part of their services.
  - The use of wearable data for targeted advertising has been tried, but not flourished.
  - Data from consumer devices offers huge potential benefits to providers and consumers. However, there is a lack of clarity around many aspects of how data is shared between consumers and the providers that serve them, which creates risks and reduces value for all stakeholders.

In short, the market for Health and Wellbeing data is large, rapidly growing and complex. Looking to the future, sensor technology which is under development today offers the potential to greatly expand the scope and power of Health and Wellbeing services. There is a big push to integrate non-medical data into clinical settings, primarily focused on preventing illness – one of society's big challenges.

2. Context and Market Trends.

The rise of the "quantified-self" movement over the last decade has seen a boom in user-generated Health and Wellbeing data from apps, sensors and wearables. This trend will accelerate with a forecast CAGR of 40% from 2020-2050[3]. Future developments in sensor technology look set to power this growth in the coming decade, unlocking value opportunities based on biomarkers, mood sensing and brain activity.

2.1 Scope and segmentation

We suggest a definition of Health and Wellbeing data and that the market can either be segmented by the type of sensors that collect the data or the purpose for which the data is used.

There's no formal definition of the digital "Health and Wellbeing" market that we are aware of, so we will define what we mean by it in the context of this report to be:

> *" Data that consumers generate by using their digital services and devices, outside of a clinical setting, that supports their Health and Wellbeing."*

For clarity, this definition excludes medical devices but includes devices or apps given to the consumer by third parties to monitor their activity for their mutual benefit e.g., a location tracker for a person at risk.

Technology

Within this market, there are three means by which the data can be captured:

- Personal wearable devices
- Environmental sensors
- Monitoring software

The first of these groups represent hardware devices carried by the consumer e.g., Fitbit. The second is hardware devices embedded in the consumer's environment, whether by them or at their behest e.g., home monitoring. The third group is software that the consumer installs on their device, to collect and/or aggregate data about them.

This third group includes physical and mental health apps, dieting apps, step counting apps and reporting functions such as Apple's "Screen time". Such software may be intended solely to provide the consumer with insights or may be provided by a third party to enhance a broader service that the consumer has purchased from them e.g., an insurer offering lower premiums for the active.

Segmentation of today's market

To understand the market trends and size we have identified a set of distinct market segments. Considering the technologies above highlights the range of capabilities encompassed by our market definition. However, it is a poor basis to segment the market and understand size and trends. Segmentation is best done on the basis that companies within a market segment should have a degree of substitutability between each other. Based on our review of the market as it exists today, we have identified the following distinct market segments covering the majority of the value generated today:

1. Diet and Physical Health apps
2. Mental Health apps
3. Health and Wellbeing wearable devices
4. Home monitoring
5. Targeted advertising
6. Insurance

The following section examines the commercial size and trends within these segments.

3 Berkshire Hathaway, 2020, UK Wearable Sensor Market Trends and Forecasts to 2025.

2.2 Market Size and Trends

We are seeing growth both in the depth and breadth of Health and Wellbeing data being generated, with significant activity across all segments of the market. However, no really sustainable data business models have emerged, with experiments around models such as advertising proving unsuccessful to date.

2.2.1 Diet and Physical Health apps

In 2017 there were over 318,000 Health apps in Apple's and Google's App Stores. However, only 41 Apps had more than 10m downloads which accounted for almost half of all downloads[4].

In the UK, the health and wellbeing app market was worth £1.3Bn in 2018[5]. With 66% of UK adults having downloaded a mHealth app. The NHS has made some steps to help consumers identify the most effective apps by offering recommendations for 72 mHealth apps[6].

Randomised Controlled Trials have shown digital apps can offer tangible benefits for conditions such as pulmonary rehabilitation and diabetes. This has led to recommendations that such consumer apps be used in clinical pathways. Such evidence combined with an increasing percentage of healthcare spend migrating to preventative support is leading to an increasing blurring of the line between "consumer wellbeing" and "clinical interventions"[7].

This trend is also evident in the current reform of the NHS and Social Care, which mandates the creation of Integrated Care Systems (ICS) which use data sharing to integrate the provision of services by a range of actors including the NHS, Local Authorities, pharmacies, charities et al. It is envisaged that these data systems will enable the ingesting of user-generated data from consumer wearables to add context to clinician's decision making. Today the NHS spends about £5Bn a year on health-related digital infrastructure, going forward a part of this expenditure will focus on the creation of ICS's.

2.2.2 Mental Health apps

It is estimated that over 10,000 mental health-related apps are available on the market[4]. Some of these, especially those focused on techniques such as CBT, can be as effective as pharmaceutical-based interventions. The range of issues mental health apps seek to address include:

- Anxiety
- Seasonal Affective disorder
- Bipolar disorders
- Psychotic disorders
- Eating disorders
- Obsessive compulsive
- Phobia
- PST
- Suicidal ideation
- Addiction

Mental health problems account for about 50% of all health issues in the under 65-year-olds in the UK[5]. Just over half of NHS GP referrals wait 3 months or more for an appointment[8]. A landmark report commissioned by the Prime Minister in 2017[9], found 15% of workers to be suffering from a mental health issue. 300,000 of which would lose their job due to this issue each year. The net cost to the UK economy was estimated to be between £72 and £99bn annually.

The digital mental health app market is rapidly growing to meet the significant untapped demand. Global Market Estimates forecast that the mental health app market will grow with a CAGR of 23% between 2020 and 2026[10] Albeit from a modest global market size of about £500m in 2018. We note some estimates for the global market size are as high as £3bn, which may be due to differences in their definition of mental health and wellbeing.

However, a 2019 study by Privacy International[7], demonstrated significant data sharing between mental health apps/websites and predominantly advertising 3rd parties. In some cases, this included those apps participating in programmatic advertising and so the use of the app/site being appended to broader user-profiles and distributed to hundreds of advertising brokers.

4. IQVIA Institute for Human Data Science: The growing value of digital health in the UK (2017)
5. Global Market Insights: mHealth Report ID: GMI286 (2019) : https://www.gminsights.com/industry-analysis/mhealth-market
6. Medtechlive 31st July 2020: https://www.med-technews.com/medtech-insights/the-burgeoning-mental-health-app-sector/
7. https://privacyinternational.org/report/3351/mental-health-websites-dont-have-sell-your-data-most-still-dohttps://www.imperial.ac.uk/business-8. school/blogs/alumni/digital-health-transforming-mental-health-treatment-the-uk/
9. *Farmer and Stevenson (2017). Thriving at Work: The Independent Review of Mental Health and Employers. UK Government*
10. https://www.globalmarketestimates.com/market-report/global-mental-health-apps-market-2192

2.2.3 Health and Wellbeing wearable devices

Wearable devices have moved from niche products to a mass-market category in just a few years mainly due to the widespread adoption of smartphones and the rise of the so-called quantified-self movement[11].

For the past 5 years, the UK wearables market has seen a steady growth in sales, driven by both growing adoption and replacement demand. In 2022, shipments of wearable devices will reach 9.6 million units, growing at a compound annual growth rate (CAGR) of 11% between 2017 and 2021.[12]

Smartwatches will be one of the fastest growth categories over the coming years. Replacement devices will be responsible for two out of three smartwatches sold in 2022. The 'quantified self' category will remain the largest by volume, at 5.4 million units. Of these, fitness trackers will fall to 2.6 million, and sports watches will deliver just 0.3 million units, as both product categories come under pressure from smartwatches. On the other hand, smart hearables will grow to 2 million units in 2022, and smart sports shoes will reach 0.4 million units.[13]

The range of functionality offered by wearable devices has significantly increased over the last few years. Heart rate sensors have become the norm. High-end devices such as the Apple Watch now also offer the ability to measure blood oxygen levels.

Another emerging trend is wearables offering the user the ability to measure their mood. The UK early-stage business "Moodbeam" enables its users to log their mood via buttons on the device. Meanwhile, Amazon's Halo devices use analytics to characterise the user's mood and tone of voice. By plotting our voice on a simple matrix of energy vs positivity, it encourages users to aim for a "calm" sweet spot. Deloitte's in-house magazine suggests that this could be used as a workplace tool, alerting HR if an employee is overly negative and energetic with co-workers[14].

2.2.4 Home monitoring

Home monitoring comes in a variety of forms, ranging from devices that monitor and support the vulnerable to fully sensor-equipped homes empowering a "quantified life".

Today the market for solutions to monitor the vulnerable encompasses call-assist for the elderly, medication management and wandering management. The global market size is about £4bn[15] and is set to grow as the population ages and more emphasis is placed on keeping the elderly in their own homes for as long as possible.

Another value opportunity for home monitoring may be driven by more people wanting to adopt an environmentally friendly lifestyle. Home monitoring can enable the individual to understand their energy consumption, use of products and thereby understand and adapt their behaviours.

Note, we have not considered home security systems or clinical systems to monitor patients at home here, as both are outside the scope of this report.

2.2.5 Targeted advertising

The advertising ecosystem is always hungry for data to target their adverts. Many Ad platforms have seen wearables as an enticing new source of data and responded accordingly, with rather mixed results.

The leading ad agency Mindshare (Group M/WPP) created a "wearable technology unit" in 2014 called Life+. This unit formed strategic partnerships with wearable manufacturers to create an environment where client brands could understand the capabilities and value opportunities of wearable devices. Today, they have an end-user cohort that uses wearables and shares their data with Mindshare to create aggregated insights for business clients.

The sports apparel company Under Armor spent c£500m between 2013 and 2015 buying MyfitnessPal, MapMyFitness and Endomondo for $700m. Its motivation was to connect the brand directly with customers, creating the opportunity for the brand to understand and engage its customers, deepening the customer relationship. This also opened the opportunity to connect 3rd parties to their customer base via an ad network. Once heralded as the core of the company's strategic growth, Under Armor divested two of the apps in 2020 and no longer sees apps as a primary revenue driver. This reflects a fading of the advertising industry's hopes that consumers would embrace using Health and Wellbeing data to target adverts.

11. Centre for Digital Democracy, 2017, Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection.
12. CCS, 2018, Market Forecast Wearables UK 2018-2022.
13. Berkshire Hathaway, 2020, UK Wearable Sensors Market Trends and Forecasts to 2025.
14. Financial Times, 2019, Data brokers: regulators try to rein in the 'privacy deathstars'.
15. https://www.globenewswire.com/news-release/2018/10/11/1619787/0/en/global-market-for-elder-care-technology-to-reach-13-6-billion-by-2022.html

Looking to the future, it is likely that increasingly assertive enforcement of GDPR by the regulators will make targeted 3rd party ads using wearable data a difficult model to scale, especially given the granularity of user consents required. In its existing form, we do not expect this business model to grow, but other, more consumer-centric models, such as "intent casting" leveraging wearable data could potentially take its place.

2.2.6 Insurance

Disruption in the insurance market driven by digital data seems inevitable and, in some categories, already recognisable. This is especially the case in Life Assurance. The outcome of this disruption will significantly define the future value boundaries for Health and Wellbeing data for all stakeholders.

The insurers' ability to persuade their customers to share more data with them appears to be critical to mitigate this disruption.

Two-thirds of the £72bn collected in UK insurance premiums annually are for life assurance[16]. More than 30% of insurers worldwide are using wearable technology for customer engagement. The table below provides examples of UK insurers using the technology to incentivise policyholders.

The insurance industry uses data generated by wearables to both provide customers with personalised information on their behaviour and to support their core insurance business (see figure 1).

> *"By monitoring a person's habits, lifestyle and surroundings, significant amounts of personal data can be collected, with permission. The analysis of such data could be employed by insurers to provide products that are tailored to the individual."* source: Allianz, 2017

Such data can be used by insurers to:

- Improve pricing/risk models
- Reduce claims by promoting healthy lifestyles
- Differentiate product offers
- Deepen customer relationships

The centrality of data in insurers' business models means that they are likely to face new competition from two directions:

1. Manufacturers of connected devices bundling in insurance e.g., Tesla offering car insurance or Babylon health insurance.
2. Consumer brands who hold broader data assets move horizontally into insurance e.g., the tech giants.

Examples of wearables in insurance products

Aditya Birla Health Discounts for policyholders who record a specified number of steps using an activity tracker or attend gym sessions or have a health assessment.	**The Vitality Programme** Vitality members earn points and achieve a higher Vitality status when they undertake activities that are assumed to impact on health status. Higher Vitality statuses unlock higher rewards for benefits such as gym, travel and other discounts.	**AXA** Offers a free Withings Pulse fitness tracker. Participants receive discounts of over $100 on their insurance policies, as well as discounts off any Withings product purchases when they complete a certain number of steps.
Oscar Rewards customers who track their fitness data gift cards when they reach their step goals.	**United Healthcare** Rewards users with healthcare credits for reaching daily fitness goals.	**Qantas Assure** Policyholders receive Qantas frequent flyer points if they lead more active lifestyles.
Aetna Monitors daily activity and provides assistance in achieving personalised health goals. The app also provides recommendations, nudges and rewards.	**Esurance** SavorBand devices are offered which can capture information on food consumed, including recipes, cooking tips, and purchasing discounts along with other data.	**Beam Technologies** Uses Bluetooth-enabled toothbrushes to reward good brushing habits with discounted insurance premiums and other rewards.

Figure 1: examples of wearables in insurance products

16. https://www.ibisworld.com/united-kingdom/market-research-reports/general-insurance-industry/

2.3 Innovation and R&D

Investment in data-driven Health and Wellbeing innovation and R&D further emphasises the critical role of ethics and governance in the fair and successful flow of value for all stakeholders, enabling opportunities to address big societal, Health and Wellbeing challenges facing all countries over the next period.

Three areas of R&D that are just starting to make their way into innovative wearables products are the measurement of:[17]

1. **Emotional states**

   This is typically done by collecting voice or facial expression data. Vendors include Beyond Verbal, Affectiva, Realeyes and Sticky.

2. **Biological states**

   This is typically based on biomarkers released in sweat or breath. Currently, the tech is at the trial stage. Vendors include Glucowise and Epicore.

3. **Brain interfaces**

   These can either utilise invasive or non-invasive sensors. Progress in the field is rapid, with the first human trials of non-medical products due this year.

All of these technologies are likely to enter the mass-consumer market over the next decade. They will herald a very different world. Imagine a world in which:

- The advert I am watching evolves differently depending on my facial reaction.
- HR is alerted if I get angry at work.
- My training shoe manufacturer says they're concerned I may have diabetes.

Now imagine the impact on a vibrant service innovation market offering choice and healthy competition, value and fair outcomes for consumers if the above were provided by a single private company.

Before leaving the Innovation topic, it is worth turning our attention briefly to the OODA loop. Developed by the US Colonel John Boyd in 1950's, the acronym stands for "Observe-Orientate-Decide-Act". Essentially in a military context, if you can execute this loop faster than your adversary, then you can act and so change the facts on the ground (or air!) before they have formulated their action plan, rendering their plan outdated.

Why is the above relevant to this discussion? Machines that are informed by wearable data may be able to execute the OODA loop faster than humans. They can already perform many types of calculation faster than us, but today are slowed by the need to acquire relevant data when interacting with humans. Wearables hold the prospect of closing this gap.

What's the consequence of this gap closing? Potentially it may lead to us not only not knowing the aim of a system we are interacting with, but also unable to decern its aim by observation alone. Imagine an advertisement to promote cigarettes, that doesn't want us to know it's an advertisement. Each time we start to suspect that's what it is, it changes direction, to throw us off the scent. Its message could impact us without us decerning when that occurred. Interacting with a system whose purpose is unknown, denies us the ability to apply critical filters, and leaves us vulnerable to influence.

Ethics and governance are every bit as, if not more important than technology when considering how best to mature industries founded on the sharing of user-generated data.

17. https://www.cambridge.org/core/services/aop-Cambridge-core/content/view/56919A6812F5439BD4C49AC758C7CE63/S1357321719000072a.pdf/div-class-title-wearables-and-the-internet-of-things-considerations-for-the-life-and-health-insurance-industry-div.pdf

3. Perspectives of Market Participants

3. Perspectives of market participants.
Key Takeaways

There are multiple stakeholders that are likely to benefit, and/or be disrupted by, the use of Health and Wellbeing personal data. In this section we will look at the opportunities open to them and some of the apparent risks they face, which for some, could have devasting consequences.

- There is an opportunity to shape the market toward a fair value exchange as no dominant winners of the Health and Wellbeing ecosystem have yet emerged.
- However, Big Tech holds many of the key capabilities needed to dominate the market, although lack the consumer's trust to exploit this position.
- The UK health sector, being 9% of GDP, has been slow to digitise, but doing so is critical to increase wellbeing and prevent illness, and more effectively care for the sick, while maintaining or reducing costs.
- Insurers are using Health and Wellbeing data to better estimate risk and collaborate with customers to mitigate risk and costs. However, slow transformation leaves the insurance market open to disruption. Tesla's recent use of car data to enter the insurance market offers an analogous example.
- New consumer-centric approaches to data sharing enable technology companies to innovate new products, which in turn could negatively impact other types of tech companies such as electronic health record companies.
- Today's practices risk consumer harm from personalised pricing and bias. Tomorrow consumers may face additional harms from manipulative AI and abuse of consented remote monitoring.

There is an immeasurable loss of value across all markets and stakeholders caused by consumer mistrust about how their data is being processed and shared. The Health and Wellbeing market is fragmented and the lack of transparency in some quarters risks a health 'Cambridge Analytica' moment, the consequences will set back value creation opportunities for our consumers, businesses and society. A number of sectors are increasingly impacted by Health and Wellbeing data, but awareness of this varies, leading to some sectors being underprepared.

3. Perspectives of Market Participants.

The Health and Wellbeing ecosystem is comprised of layers of data producers, enablers and services that use the data. No open ecosystem or dominant market makers have yet emerged, creating an opportunity for new value creation across the entire Health and Wellbeing market. The tech giants are in a strong competitive position, with implications for the 3rd party services that are / will be dependent on Health and Wellbeing data. However, Big Tech suffer from trust issues which impacts their ability to act freely in markets and gain and maintain consumer trust in the supply of services.

3.1 The ecosystem and market dynamics.

Layers in the ecosystem

The emerging ecosystem which captures and creates value from user-generated Health and Wellbeing data can be thought of as consisting of four layers (See figure 2). The ecosystem rules and market structure determine how the data flows between the layers and the degree of trust the consumer has in these flows.

In the first layer is the consumer who makes the action which is described by the data. The second is the device or sensor that measures the action and turns it into data. The third layer comprises enablers that add utility to the data, be it data networks transporting it to the right places, or legal firms creating trusted contractual frameworks. The final layer encompasses the service providers who create value from the data. Many ecosystem participants act on more than one layer.

Many services originated as single-function services e.g., to track step counts or log diet. However, over time they have tended to broaden in scope e.g., monitoring heart rate or encompassing a social network for runners.

This evolution has increased the scope of data they capture. In turn, this could enable more 3rd party services to create additional consumer

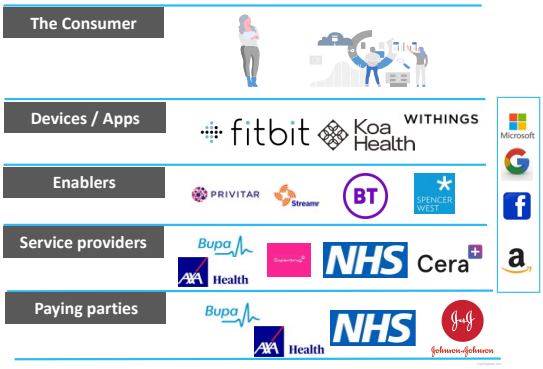


Figure 2: layers of the ecosystem

value from the data e.g., insurance companies or health providers. To increase the consumer attractiveness of the original/primary service, interfaces have been created to "walled gardens" of 3rd party service providers. However, the growth of these 3rd party ecosystems has been slowed by:

- Concern about consumer perceptions of data sharing
- Fragmented market means most parties lack the scale to attract/sustain 3rd parties
- Limited internal innovation bandwidth
- Relatively weak incentive structures

The GAFA (Google, Amazon, Facebook and Apple) are in a different position, as they have scale and span the ecosystem's horizontal layers. This opens the possibility for them to create vertically integrated solutions and developing 3rd party ecosystems at scale.

Such a strategy would align well with their declared interest in healthcare and place them in a strong position commercially with organisations that want to join their ecosystem to access "their" customer base.

Consumer Attitudes

If we look at consumers' attitudes toward sharing their data, over half express significant concerns about how their data is processed and shared. These reasons are predominantly related to trust issues. Consumers don't understand what companies are actually doing with their data. Consumers also don't trust companies to follow their stated policies.

Very broadly, about 30% of consumers are comfortable sharing their data, 30% are neutral with some concerns and 40% are uncomfortable with significant concerns[17b].

By addressing this, a sharper line of demarcation would be created between the "data-generating" service and those services which benefit from using data generated.

This may act as a prelude to a standardised interface that would drive the scaling of an open ecosystem. Such developments are critical if service providers (e.g. health and insurers), who are dependant on such data flows, are to retain access to the data without becoming dependant on the tech giants.

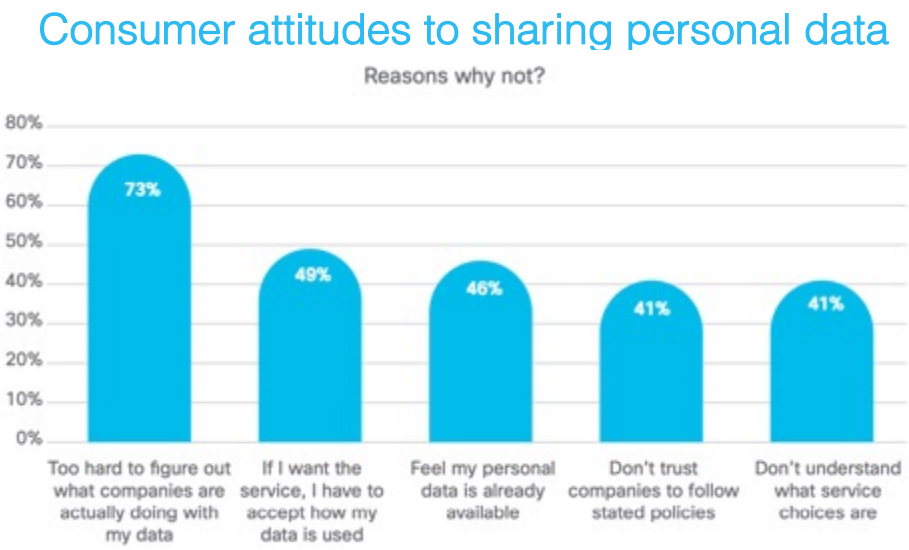


Figure 3: Consumers' reasons not to share their data
Source: Cisco "Consumer data privacy report 2019

"Lock-in" limits value creation

The data generated is increasingly rich and can support a diversity of services. To maximise value creation for the consumer, wearables need a way to share data with many other service providers who can support the individual in different ways, while preserving the individual's trust and preparedness to use the wearable device.

To achieve this the customer needs certainty that the data would only ever be used in their interests and under their effective control.

What appears missing is a technical framework, liability and governance models to enact consumer control and anchor consumer trust.

3.1.1. The Health Provider's perspective

While the last decades have seen the partial digitisation of healthcare, it has yet to become systematically integrated via data flows between organisations. Such a pivot is necessary to make health, social and wellbeing work seamlessly together.

Health Provider market

Healthcare is a big business (8.8% of GDP for OECD countries, 8% for the UK, up to 16.9% for the USA) and is still slow on the digitisation front. Shifting demographics and especially the ageing of the population is a real threat to current systems.

[17b] https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

These strains are amplified by COVID, with more hospitalisations and Mental Health issues emerging. For instance, employees are three times more likely to have Mental Health episodes under current lockdown.

There is widespread understanding that the current primary, secondary and tertiary layers of healthcare provision, first conceived in the 1930's need to change. Between 1950 and 2019, the NHS's budget has grown from 3.5% to 7.3% of the UK GDP (source: Nuffield trust).

A part of the solution that appears to be widely accepted is to redeploy resources from "fixing the sick" to "keeping the well, well". At the heart of this vision is the use of data to support the healthy and co-ordinate and tailor healthcare providers efforts to individual needs. The UK Health of the Nation Report estimated that increasing the percentage of health expenditure on preventative measures from 5% to 15% would add five years of additional healthy life to the average life span.

The flow of both health provider and user-generated data between all parties is critical to achieving this vision. This nexus represents a huge commercial opportunity for all players, especially the Tech Giants.

Enter Big Tech

The tech giants (GAFA – Google, Apple, Facebook and Amazon) can leverage scale and their large active user base, their brands are strong, and they are known for delivering a strong customer experience.

Furthermore, they are cash-rich and make acquisitions (Fitbit acquired Google, Amazon launches and acquires pharmacies and clinics, Apple is launching clinics and working already along the continuum of Health). All GAFA have ambitious Health Strategies and are starting to implement them. Wall Street analysts forecast Apple will generate $350B annual revenue from Health by 2027 (13 times the total revenue of AstraZeneca and 11x GSK's).

Issues for roll-out and scale-up are two-fold: 1) GAFA are not tailored to produce medical-grade equipment (yet). Healthcare providers and Insurers in the US complain the Apple watch has too many false positives detecting heart fibrillation, thus increasing unnecessary emergency wards visits.

2) Trust. Facebook is obviously the usual suspect, but Google does not fare better: In November 2019, a whistle-blower revealed that in Project Nightingale, Google received from a major US healthcare provider, the personal Health data for up to 50 million Americans, including full personal data, identity and medical history, without warning being given to patients or doctors.

Consequently, the threat to existing healthcare providers is that they become dependant on the GAFA, potentially increasing costs and limiting innovation and market access.

3.2 Market participant perspectives

3.2.1 The Consumer's Perspective.

Consumer mistrust about how their data will be processed and shared may be impeding the growth of the digital Health and Wellbeing market. This represents a loss of value to both consumers and businesses.

Consumer attitudes to adoption

While 90% of people say they would be happy to use a wearable device prescribed by their doctor, only 28% would trust a consumer device e.g. Apple or Fitbit (source: Fierce Health 2020). Reticence is born of both accuracy and privacy concerns. Addressing these concerns could expand the Health and Wellbeing market and unlock individual and societal benefits.

3.2.2 The insurer's perspective.

Insurer's businesses are founded upon an asymmetric information advantage. Their ability to predict risk from personal attributes in part shapes their profit margin. As such their businesses are contingent on access to the right data. To date, the industry's adoption of user-generated data has been patchy. The insurance market is increasingly looking ripe for disruption.

The initial adoption of user-generated data sources

Traditionally insurers assembled data at the point in time a potential customer sought to take out an insurance policy. This data was acquired both by asking the consumer and via private B2B data transfers to the insurer. Policies were generally static with risk and pricing determined at the start and fixed for the policies duration.

The last decade has seen a growing use of dynamic data captured by sensors during the policies lifespan and the product applying rewards and/or penalties in response to changes in risk inferred from the changing data. Examples include accelerometers attached to cars to dynamically price car insurance and wearable devices to price health insurance.

Philosophically these developments have seen insurers evolve from underwriting loss, toward loss prevention. United Healthcare in the US estimates that each individual using their tracker programme costs them $228 less in health costs per year (*source: FT 2019*). The benefits to both the insurer and consumer of avoiding illness are significant.

Disruption is on the horizon

The arrival of data mobility is a mixed blessing for insurers. On the one hand, it unlocks powerful new sources of predictive data e.g.:

- Changes in mobile phone calling patterns can be used to identify the onset of depression.
- Changes in vocabulary in email can indicate brain degeneration.

Yet on the other hand sizable parts of these new data sources are already held by the tech giants and data mobility enables them, if the consumer gives consent, to acquire the remaining pieces.

> *"We're undertaking an International transformation and need to understand the impact and opportunity that personal data has on the health landscape and that transformation."*

Source: a large health insurer

There is a very real prospect of insurers going from an information advantage to a disadvantage. This is compounded by the internet giants actively making or acquiring wearable device brands. Making sure there are frameworks for trusted data flows, which are trusted by consumers to enable them to consent to insurers accessing this data, is a precondition for insurers to achieve a level playing field vs tech giants who enter the insurance market.

3.2.3 Supporting services and tech providers perspective.

There are many facets to creating flows of data that are trusted by consumers. Technology, consent, privacy communication, audit, governance and liability models are all required. For a host of technology and professional service companies, the rise of trusted data flows represents a new market opportunity.

Technology

A range of new technologies can contribute to the creation of trusted data flows. These include data facilitators to give users more control over the sharing of the data. Consent receipt technologies to ensure the integrity of the consent records. Privacy-preserving technologies such as homomorphic encryption and federated learning. Consequently, the tech sector is interested in this issue, not least as from a technology perspective it mirrors likely developments in other verticals, which collectively represent a large market.

> *"We've been looking at the data empowerment of the individual for over a year and how that changes the Health Landscape."*

Source a big tech company

However, for systems integrators, the picture looks less healthy. By aggregating the data under the consumer's control, it enables a simple way for multiple parties to access that data. This threatens a significant part of the SI existing revenue streams.

Professional services

In addition to new technology opportunities, the creation of trusted data flows opens new opportunities for law firms and auditors.

A significant part of the challenge in enabling trusted data flows lays in creating the right governance and liability structures. Associated with these there needs to be dispute resolutions mechanisms.

Trusted data flows also require participants to adhere to a set of rules and standards. It may be the case that to build consumer trust that the rules are being adhered to requires regular audits.

These all represent new commercial opportunities for professional services firms.

3.3 The case for change.

The Health and Wellbeing data sharing ecosystem has several gaps and structural issues, which lead to potential consumer harms. Current trends seem likely to exacerbate this.

3.3.1 Gaps

Today there appears to be a number of elements missing from the Health and Wellbeing data market that one would expect to see in a healthy end-state market.

Consumer trust in data: is lacking and we will explore this in more detail in the later sections of this report. But we would expect to see a robust data sharing governance system which is clearly articulated to the end consumer.

Open ecosystem of APIs: Today consumers are not fully empowered to share their data with all 3rd party service providers. Barriers range from friction caused by poor user data sharing experiences to, in some cases, a lack of interoperability.

Open data training sets: It's hard for innovators to fully appreciate the value that they could create with Health and Wellbeing data without access to it in an anonymised form to build models. Such open/semi-open training data sets seem missing.

3.3.2 Structural Issues

Given the huge scale of the Health industry, there appears the risk that the wellbeing data market becomes a tail that wags that dog.

As the tech giants move into the health market, they may acquire consumer Health and Wellbeing services to complement their Health Services. This will then embody their respective competitive Health strategies into the wellbeing data market and may balkanise it, destroying consumer value. Further, this may impact the insurance industry which does not appear fleet-of-foot in acknowledging the growing threat to their market position.

3.3.3 Potential consumer harms

Further issues and potential consumer harms may arise from the use of Health and Wellbeing data to underpin health and life insurance. We expect some digital Health and Wellbeing companies to leverage their data to enter the insurance market. This high degree of personalised pricing will enable them to attract only the most profitable customers. The pool of customers remaining will then be higher risk than conventional insurance data models suggest. The resulting initial financial hit on the traditional insurance industry is likely to result in a rise in insurance premiums for those not using digital Health and Wellbeing services. This will constrain consumer choice and ability to risk pool. This "disaggregation" of the insurance market will leave the most vulnerable facing prohibitively expensive premiums, undermining insurance's very model of distributing the risk.

Finally, potential consumer harms may result from a lack of clarity about how a premium was set, leaving open questions about bias and discrimination.

3.3.4 Potential Future Consumer Harms

While many of these value opportunities offer exciting ways to improve the lives of consumers, many also open new sources of potential harms, over and above those mentioned in the last chapter of this report. Two concerns are 1) the introduction of real-time human to machine feedback loops and 2) the increased surveillance of employees by employers. The following looks at these in more detail.

3.3.5 Manipulative AI

As discussed at the end of the "Context and Market Trends" section, the emergence of mood sensing technologies and brain-machine interfaces, for the first time, pits humans against AI in real-time. This is qualitatively different from the use by Cambridge Analytica et al using AI to select static adverts.

For example, imagine being shown a personalised advert employing some mood sensing technology (say based on facial expression). The advert's narrative could evolve differently depending on your emotional response to it. Such an advert would be manipulating the viewer in a way that would be hard to perceive.

Digital systems are highly scalable and programmatic advertising campaigns interweave their way through the internet's digital inventory, making their content hard to escape. Further, the "logic" of AI algorithms is often opaque, making governing AI impossible.

In a world beseeched by digital echo chambers and political polarisation, the impact of such developments on our already fragile concept of "free will" may be concerning. More research on "the dynamics of complex networks" to detect such manipulation would seem an important and urgent topic. While it is undoubtedly hard to hold back innovation of such powerful techniques, it may be that the solution to such data-enabled challenges lays in the data itself and our ability to construct monitoring methodologies to identify emerging harms.

3.3.6 Surveillance of employees

"Stay at Home, Protect the NHS, Save Lives", is a slogan fresh in the mind of anybody who visited the UK in 2020. And stay at home we did, with mass working from home continuing into 2021. A slew of companies have since announced that they don't intend ever returning to the 5-days a week office-based work pattern. This carries a number of implications. If staff feel isolated, depressed and/or suicidal, to what degree is that the employer's responsibility? Are they obligated to look after their staff regardless of their location?

On the other hand, how does the employer know their staff are actually working at home? Many employers may feel these considerations necessitate that they monitor their staff's activity at home. This is leading to laptops becoming a form of "Health and Wellbeing" data-generating devices, with staff mandated to share that data with employers.

However, what's being monitored? Is it just the time you spend at a keyboard or are your keystroke patterns being monitored to detect if you are hungover? Or your voice tone monitored to score you against conformity to the corporate "Values" statement? In short, what level of intrusion does an employer have a right to ask for by virtue of employing someone?

There would appear to be considerable scope to harm of employees' mental wellbeing by overly intrusive employers. Yet today this area is thin on applicable ethical codes and the relevant laws were not designed with this situation specifically in mind. This would appear a topic worthy of further work, to inform the evolution of case law in the future.

Whilst this is not strictly a consumer harm, it is a harm that affects many consumers in their role as employees.

4. Value Opportunities

4. Value Opportunities.
Key Takeaways

In this section, we explore the nature and scale of the value opportunities that would be unlocked if consumers were able to share their data in a trusted way. We find value opportunities that could be underpinned by Health and Wellbeing data in nearly every sector, with the largest being in preventative care, social care and insurance.

- The generic business value opportunities that cut across industry sectors fall into three clusters:
  - Efficiency
  - Productivity
  - Innovative services
- We identify a new data-driven business opportunity to help consumers gain insights from their shared data and match their needs to service suppliers like health care providers. At their core, these businesses will offer consumers:
  - Insights, profile, persona and verified identity management
  - Personal data control and transparency tools to manage and consent sharing
- The most valuable use cases appear to be in the Health sector (e.g. preventative care), Public sector (e.g., social care) and finance sectors (e.g., insurance).
- We estimate that the scale of the above three opportunities that are enabled by the sharing of Health and Wellbeing data to be tens of billions of pounds per year in a market the size of the UK. Further, we estimate that single figures of billions of pounds a year would be directly attributable to the trust solution.
- The level of value created will be shaped by how the trust solution develops and how open, an ecosystem it leads to.

Enabling the trusted sharing of Health and Wellbeing data will shape the competitive landscape for incumbents and catalyse innovative new entrants, but ultimately, the greatest beneficiaries are healthier consumers.

4. Value Opportunities.

The trusted sharing of personal Health and Wellbeing data unlocks value opportunities across market sectors as diverse as finance to textiles. The opportunity size in a market the size of the UK is at least ten's of billions of pounds per yar. The largest opportunity is in Health and Wellbeing, where it both enables individuals to better manage their personal Health and Wellbeing, and Health and Wellbeing service providers to orientate around the individual's needs. The confluence of the burgeoning of sensor technology, the quantified-self movement and the accelerant of the COVID pandemic are combining to make now the right time to seize on these opportunities.

4.1 The opportunity landscape

4.1.1 Why now?

Technology is on the march, powered by ever more powerful computing (Moore's law) and ever faster networks (Guilder's law), the opportunity to build small powerful sensors that are always connected has blossomed over the last decade. As we have seen these can now monitor many facets of human behaviour and wellbeing and have been widely adopted. Over the last 5 years, traffic from these devices has grown 22 times.

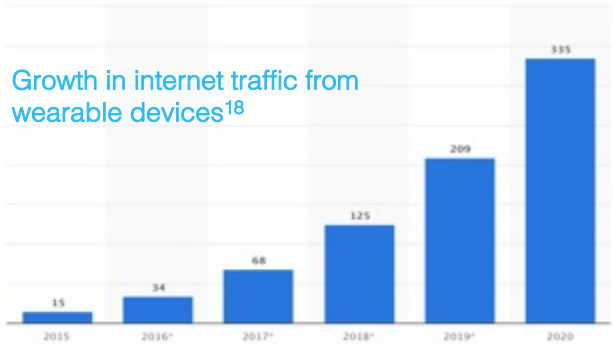


Figure 4: Growth in traffic from wearables

During the pandemic, businesses have had to learn to work differently. GPs have shifted to telephone and video consultations. Hospitals have piloted "remote wards" where patients are monitored at home. While long-COVID may lead to the need to monitor and support the rehabilitation of vast numbers of people. At the same time, people have started working from home, carrying the risk of a more sedentary lifestyle and so the need to become more disciplined about exercise. These trends combine to make the perfect storm for Health and Wellbeing services and wearable devices.

4.1.2 Cross-cutting value opportunities

Yet the opportunities to apply Health and Wellbeing data to create value exist far beyond just the Health and Wellbeing industry. By understanding where the value may sit, enables us to focus on the high value markets and opportunities across business functions, market sectors and consumer value.

Health and Wellbeing data is of value to many other industries, where it can be used to create value for both consumers and businesses. For example, in the insurance sector, it can be used to both better estimate risk and support consumers in mitigating those risks. While in the video gaming industry, it can be used to create new forms of interactive games that respond to the user's physical state. Broadly the cross-sectorial value opportunities can be clustered into three groups:

1. **Efficiency:** Where the data allows existing processes to operate more efficiently e.g. automating filling in forms.
2. **Productivity:** Where the data allows new processes to be built enriching the outcome, e.g. sharing daily heart rate with a sports coach.
3. **Innovative services:** Where the data enables completely new services e.g. mood sensing clothing.

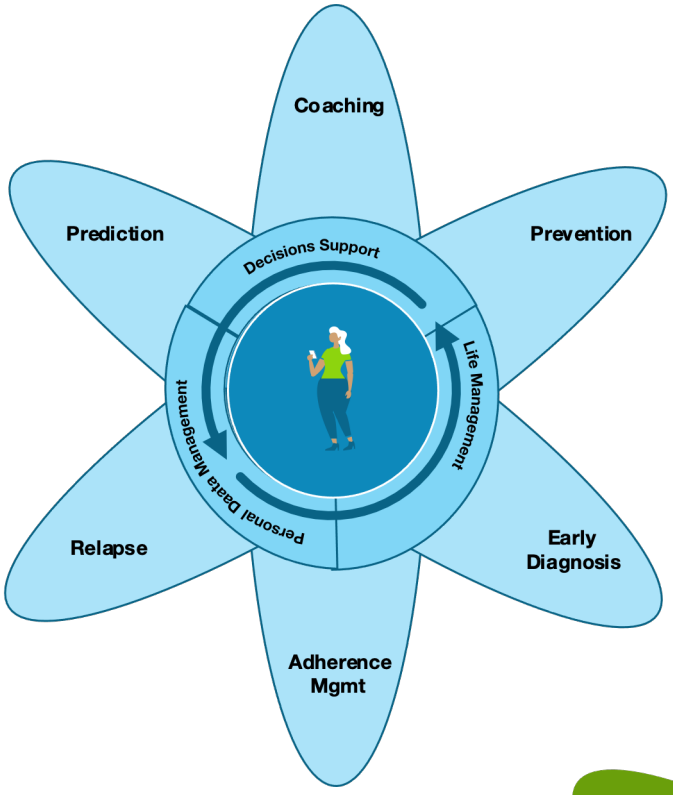


Figure 5: Consumer value clusters

Consumer value clusters

Beyond these generic value areas, sit six specific clusters of value creation for businesses and six for consumers. These are illustrated in the star diagrams below. The consumer value clusters include coaching, prevention, early diagnosis, adherence, preventing relapse and predicting issues.

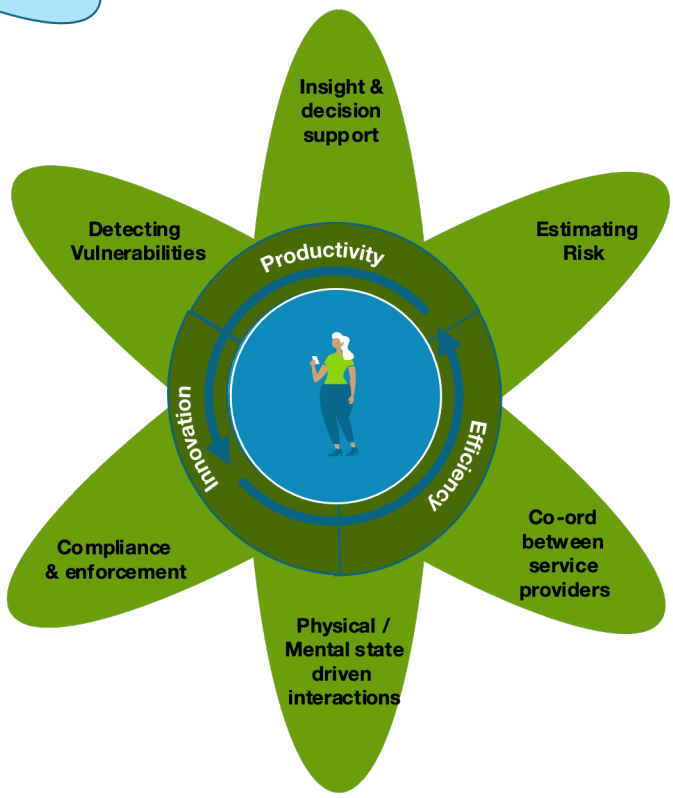


Figure 6: Business value clusters

Business value clusters

While the business value clusters include, decision support, estimating risk, coordinating between service providers, creating physical/mental state service interactions, compliance and detection of the vulnerable.

4.2 Consumer and business value

4.2.1 Improving consumers Health and Wellbeing

Consumers want to be healthy and live independent normal lives. Today they are supported in this, primarily by healthcare providers, social carers and pharma companies.

The support and interventions these organisations provide are driven by clinical data acquired by interviewing and testing patients. The collection and analysis of the data sits within the providers of these physical goods and manual services to the patients.

The creations of trusted flows of consumer Health and Wellbeing data, changes this, by creating a new market space sitting between the consumer and the providers of these physical goods and services (see figure 7 below). In this new space will emerge organisations that can build trusted data sharing relationships with consumers. This will enable these organisations to both provide digital-only services and also orchestrate the delivery of 3rd party services to the right consumers at the right time.

The emerging market structure as shown in figure 7 below potentially unlocks three transformational benefits.

- **Consumer Health:** opening opportunities for prevention, monitoring and wellbeing consumer services analysing their data to predict risks and recommend behavioural changes to avert illness. This manifests as engaging digital experiences which act in the consumers' best interests.
- **Trusted Data Flow:** The ability to access and analyse broad and deep personal data through trusted data flows to understand what services a consumer needs and when they need them.
- **Health services:** The insight to help service providers evolve and innovate new more effective services. This encompasses the development of new clinical pathways, scalable/rapid pharma trials, adherence management and efficacy proof, early diagnosis and management of relapses.

These capabilities are the fertile soil upon which new innovative services can be built. These will be critical for healthcare, pharma and social care companies to remain competitive in the new landscape. However, the value opportunities are not confined to these sectors.

This new space may be filled by existing service providers extending their business models or by new entrants organisations. It is certainly a space of great interest and activity for the tech giants.

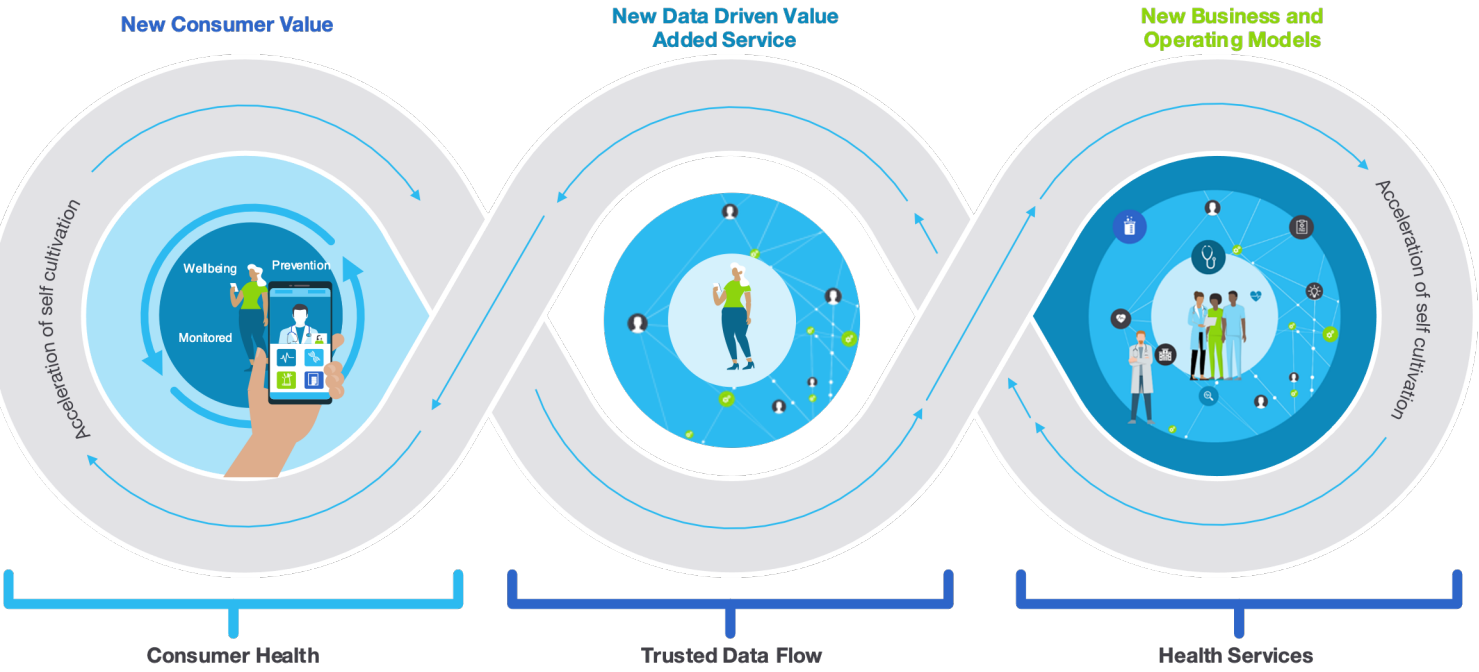


Figure 7: The emerging market structure – source: Nordic Health 2030

4.2.2 Value opportunities in other sectors

A trusted Health and Wellbeing data-sharing ecosystem can enable data to flow both within the Health and Wellbeing sector and beyond it. While large value opportunities exist in enabling this data to flow to the clinical health sector, social care sector and the insurance sector, in addition, myriad smaller value opportunities exist in other sectors.

To explore this, we took a twin-track approach.

- **Expert workshops:** Through ideation sessions, we developed initial ideas for the value opportunities in each sector. These ideas were then explored further in an expert workshop with representatives from across the ecosystem.
- **Desk research:** We estimate the order-of-magnitude value of the largest value opportunities in each sector, to get a sense of the scale of the existing expenditure on that area.

4.2.3 Value opportunities in other sectors

A trusted Health and Wellbeing data-sharing ecosystem can enable data to flow both within the Health and Wellbeing sector and beyond it. While large value opportunities exist in enabling this data to flow to the clinical health sector, social care sector and the insurance sector, in addition, myriad smaller value opportunities exist in other sectors.

18. http://nordichealth2030.org/philosophy/

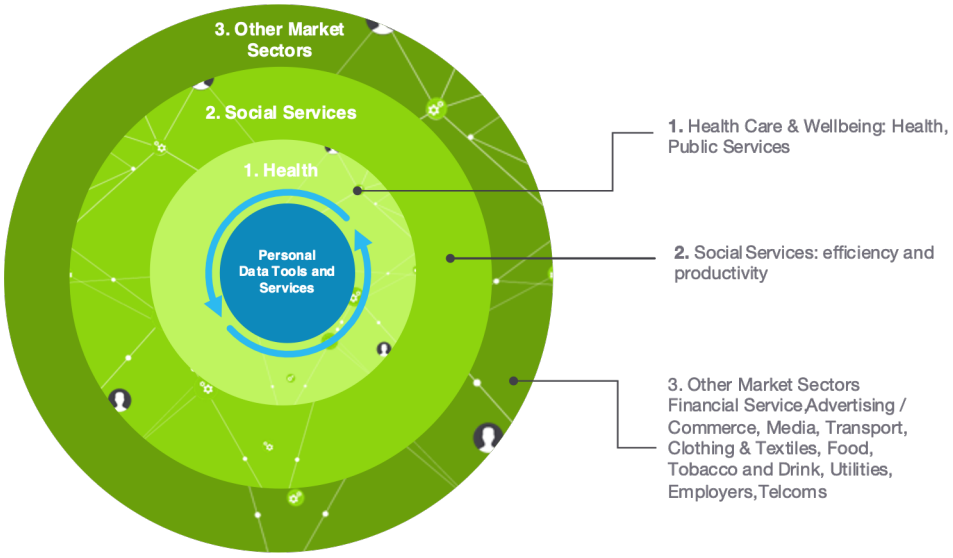


Figure 8: Market Sector Opportunities

The value opportunities that we identified from across the sectors were:

- **Health:** co-ordination of existing services and the development of remote monitoring
- **Finance:** The measurement of risk and reducing risk through interventions
- **Public services:** Social Care, monitoring for benefits entitlement/compliance and insights for planning
- **Textiles:** measuring the wearers and garments performance and wellbeing
- **Utilities:** support green customer lifestyles and identify the vulnerable
- **Telecoms:** remote monitoring services
- **Transport:** crash avoidance
- **Food stuffs:** dynamic recommendation of foods depending on wellbeing state
- **Advertising / Retail:** Targeted advertising
- **Media:** Dynamic feedback loops where the media responds to the viewer's state
- **Value to the employer:** Protecting staff and enforcing behavioural standards

The following graph illustrates the consensus views of the experts who attended the workshops on the benefits of the above value opportunities to the business and consumer. The benefits to the consumer and business are described on the following page.

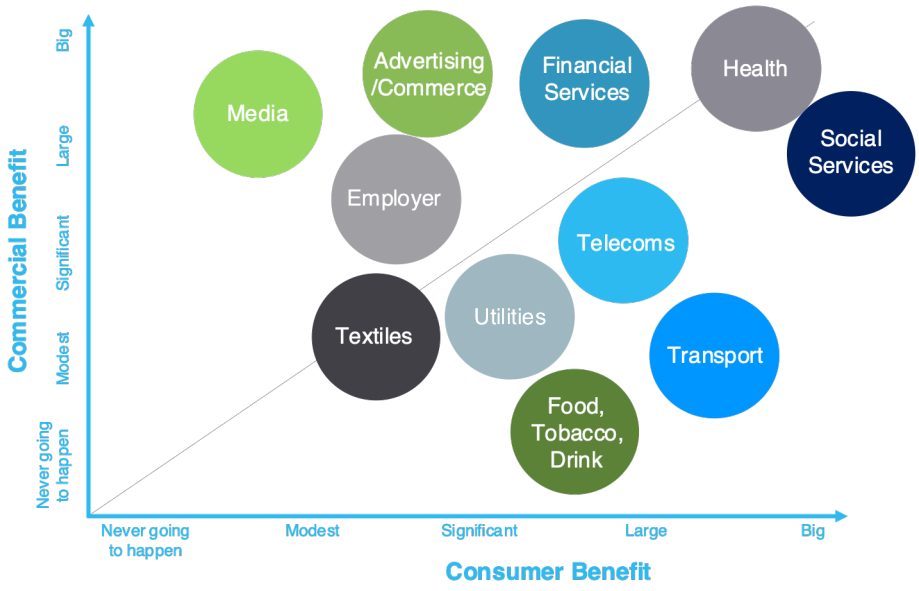


Figure 9: Relative sizes of value opportunities for consumers and businesses

Illustrative value opportunities across sectors

Sector	Business Value	Consumer value
Financial services	• Insurers (health, life): risk estimations • Credit scoring: change in health status	• Keeping healthy • Identify vulnerable customers
Public services	• Reducing social care cost through monitoring and prevention • Monitoring mobility for verifying benefits payments • Electronic tags for criminals	• Rehabilitation programmes – drugs and alcohol • Aggregate data for better public planning
Media, graphical and cultural	• Product innovation and differentiation: More compelling experiences	• Gaming in which dynamic loops of experience, link scares to physical state of player
Textiles	• Product innovation: Embedding wearables in textiles and garments - image (fashion), function, wear (shoes), health (in clinics)	• Better image (fashion), function, wear (shoes), health (in clinics)
Food, Tobacco and Drink	• Product innovation: meet new customer needs to enable change	• Help quit tobacco – transition to e-cigs • Optimise food intake e.g. Food retailers who dynamically recommend food intake – e.g. Hello Fresh
Telecoms	• Product innovation and network revenues	• Remote monitoring of elderly parents via home-based sensors • Ensuring always connected
Health	• Reduce healthcare costs by preventing sickness • Remote patient monitors: distribute virtual wards • Remote trials	• Maintain wellbeing • Joined up care – health/social etc
Transport	• Product/service differentiation	• Crash prevention – Attention monitoring
Utilities	• Product innovation: link temperature to activity	• Identify and support vulnerable customers? • Supporting customer green living
Value is to the employer	• Reduce worker sick leave, and corporate insurance • Monitor home workers via laptop • Mood and attention on Zoom calls	• Health and safety at work: tired workers on construction site • Worker wellbeing: identify emerging health issues
Advertising / commerce	• Richer targeting data: GPS, BMP/O2, Stress, Sleep • Higher click-through rates	• Relevant advertisements and opportunities
The individual	• Transparency, control and consent of of personal data sharing and use • Profile, persona and verified identity management	• Better decisions / insight • 3rd party interventions • Entitlement

Illustrations of Value Opportunity sizes

Sector	Illustrations of opportunity size
Financial services	• CRA's make about £300m p.a. from credit reports[21]. • Life and Health insurance represents about 70% of the £260bn paid in total in the UK in insurance premiums[22].
Public services	• Saving of c.£300 p.m. by remote monitoring of people in social care with a wide range of conditions[27] • Benefit fraud in UK is c£2.3bn p.a[23]
Media, graphical and cultural	• Currently use cases are not in market to size
Textiles	• Small volumes in 2020, c10m units sold globally[24]
Food, Tobacco and Drink	• Currently use cases are not in market to size
Telecoms	• Remote monitoring services market is estimated to be <£1.6bn in UK[25]
Health	• Cost to NHS of delayed discharge to social care £820m[19] p.a. • Cost to UK economy of mental health issues c£100bn p.a[20]
Transport	• The average value of preventing 1 fatal car crash in the UK is £2.2m[26]. There are about 1,800 road deaths each year in the UK.
Utilities	• Currently use cases are not in market to size
Value is to the employer	• About £200m is spent by employers monitoring staff in 2023[28].
Advertising / commerce	• UK digital advertising c£25bn p.a of which 50% is not for inventory[27].
The individual	• Each of the above also brings significant value to individual, indeed assuming a fair value exchange they should gain at least as much as businesses do.

19. https://www.sciencedirect.com/science/article/pii/S0167629618301000
20. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/215808/dh_123993.pdf
21 https://apex-insight.com/product/uk-credit-reference-agency-services-market-insight-report-2016/
22. https://www.statista.com/statistics/307942/insurance-industry-gross-written-premiums-in-the-united-kingdom-uk/
23. https://en.wikipedia.org/wiki/Benefit_fraud_in_the_United_Kingdom
24 vhttps://scet.berkeley.edu/wp-content/uploads/Smart-Clothing-Market-Analysis-Report.pdf
25. http://www.comodal.co.uk/Files/Comodal-Insight-to-industry.pdf
26 https://www.gov.uk/government/statistical-data-sets/ras60-average-value-of-preventing-road-accidents
27. https://www.worktime.com/2019-employee-monitoring-software-industry-trends

4.3 Business Opportunity Assessment

The analysis in the previous section suggests that while there are many value opportunities across the sectors, the overall value opportunity is dominated by the sharing of consumer Health and Wellbeing data for the:

- Prevention of ill-health
- Improving public services, such as social care
- Insurance services

We will now turn to explore these in more depth.

4.3.1 Prevention of ill-health

Prevention of ill health includes both physical and mental health. It comes in two flavours. Firstly, there's preventative healthcare which "keeps the well, well" and averts illness. Secondly, there's preventative healthcare which prevents relapses when an individual is being treated, which usually involves supporting them to adhere to a treatment regime.

The diagram below (figure 10) illustrates the scope and power of the ecosystem unlocked by the new trusted data sharing ecosystem. By integrating consumer data with clinical and historic data, new signals can be created, which can enable health and wellbeing across the full lifecycle from prevention, prediction, diagnosis, treatment and prevention of relapse.

We will now look in more depth at the scale of the value which a trusted data sharing ecosystem could bring to preventative care. In what follows we are not attempting to create a business case for implementing a trusted data sharing market solution. Instead, we'll try to get a sense of the order of magnitude of the value that could be liberated if the data sharing barriers were overcome.

Size of the prevention of physical ill-health opportunity

We will start with a few statistics which help us get a sense of the potential scale of the benefit:

- As mentioned earlier in the report about half the caseload on the healthcare system is from preventable illness.
- According to the eHealth ACA index report, the average medical insurance premium in the US is c.$400 or $4,800 per year in 2020. Now we saw earlier in the report that United Insurance estimated that customers who engaged with their fitness tracker programme made claims amounting to $288 per year less than they otherwise would have expected to have done. This is a 6% saving resulting from the use of wearables.

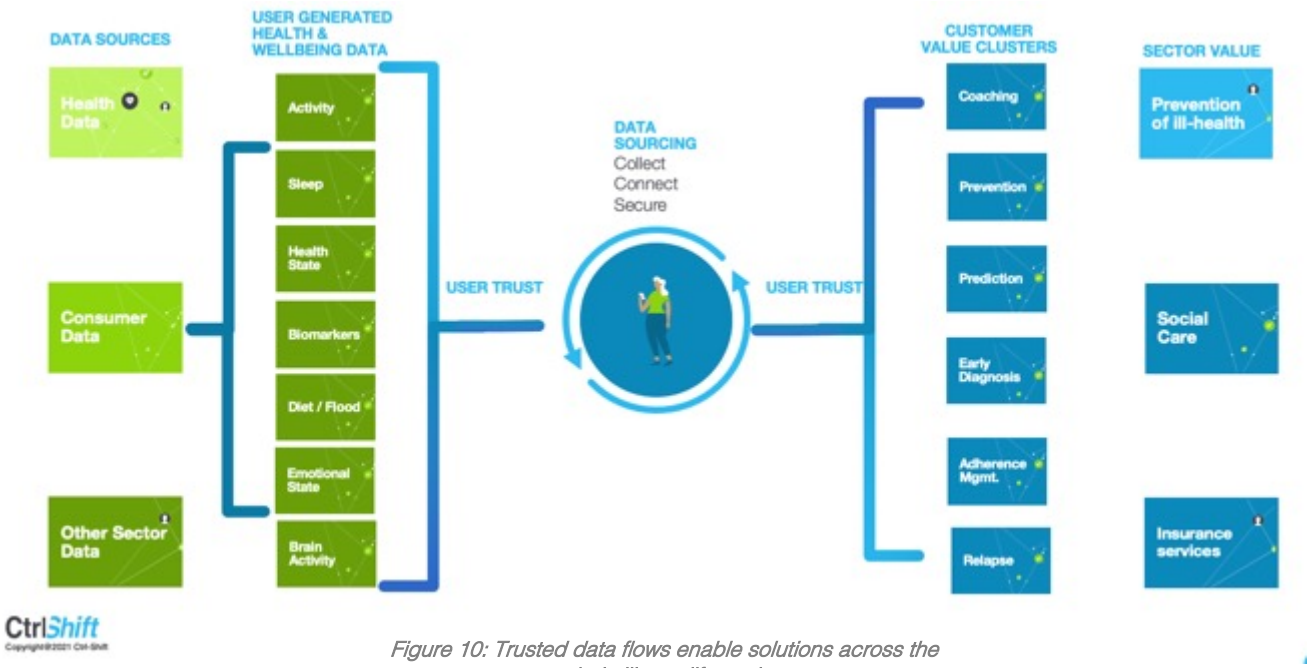


Figure 10: Trusted data flows enable solutions across the whole illness life cycle

We will now apply these insights to the NHS, whose budget is £133bn. If we take the portion of the NHS budget that pro-rata's to the preventable caseload i.e.133 x 50% we get the approximate spend on that type of illness. From United Insurance we see their programme created a 6% saving. So if everyone joined a preventative tracker based programme the saving would be:

Saving enabled by the Trust Solution:

= 13133 x 50% x 6% **= £4.4bn.**

Turning to mental health:

- We saw earlier in the report that mental ill-health costs UK businesses about £100bn p.a.
- In the US 15% of people suffering serious mental illnesses, received minimally adequate treatment.[28]
- 80% of adult mental health illness is attributable to childhood experiences and therefore predictable.[29] Each £1 spent on early intervention saves £833.
- Digital-only interventions for depression are about half as effective as conventional approaches.[30]
- About two thirds of cases with depression are amenable to treatment.[5]

So using depression as a proxy, two thirds can be treated conventionally, and about one third digitally. Today c85% receive no treatment. If depression were typical across all mental illnesses, this would imply digital treatments have the potential to address one-third of the mental health burden:

Saving enabled by the Trust Solution:

=100bn x 85% x 33% **= £28bn.**

4.3.2 Public services: Social care

With an ageing population and rising levels of ailments such as dementia, many of us will need care in our latter years. While much (c.80%) of this care is given by unpaid friends and family, the remainder is provided privately, at great cost to those individuals in care and the state. A portion of these costs is due to conditions becoming acute before they are noticed and treated. Experiments with remote monitoring in a social care setting have shown some of this can be averted thereby diminishing suffering and improving peoples lives.

Passive remote monitoring care reduces the workload on social care staff and can identify the early onset of issues with the patients, enabling interventions that avoid later costly hospital visits. The level of cost-saving varies a lot depending on the patient's conditions. Research by Schneider et al 2019, suggest savings of $425 (£300) per month for remotely monitored care pathways across a members base with a range of conditions.

- In the UK there are 850,000 receiving long-term publicly funded care. (circa 6 x this are not publicly funded)

Cost saving for publicly funded care if all were remotely monitored:

= 850k x 300 x 12 **= £3.1bn**

4.3.3 Insurance

For insurers, the sharing of Health and Wellbeing data offers the opportunity to better estimate risk, do it more dynamically and use attested data to automate more of the claims process. However from a commercial perspective, for insurers, this opportunity is more about avoiding a threat. Imagine a pool of customers who based on traditional data sources, all look to be at the same level of risk. If an insurer is slow to develop deeper data sharing relationships with customers, than competitors, they are likely to end up mispricing for risk. The reason is that as data rich competitors will poach historically mispriced customers from the customer pool (i.e. those that are actually lower risk than their "old" data profile suggests), while the slow-moving data-poor competitors will continue to take on customers from the pool without realising the spread of risks of customers in the pool has changed. This is hard to size, but as ballpark figures:

- Assume 1/3 of the life assurance industry profit pool is up for redistribution by these factors
- The UK life insurance profit pool is c.£6.6bn

Profit enabled by the Trust Solution:

= £6,600m x 33% = **£2.2bn**

4.3.4 The contribution of a "trust solution"

In the above estimations, we have indicated the scale of the value opportunity that could be unlocked in the UK by the sharing of Health and Wellbeing data. What portion of this value can be directly apportioned to the role of a "trust solution"?

28. Adequacy of treatment for serious mental illness in the United States. *Wang PS, Demler O, Kessler RC Am J Public Health. 2002 Jan; 92(1):92-8.*
29. Knapp M, McDaid D, Parsonage M. *Mental health promotion and mental illness prevention: The economic case.* London: Department of Health; 2011
30. Psychiatry, 13 November 2019 | https://doi.org/10.3389/fpsyt.2019.00759

We'll estimate this through the lens of the adoption of wearable technology.

- According to a survey by TRUSTe in 2020, 82% of Americans cite privacy concerns as a top 3 reason not to buy wearables.
- According to Statista, currently 32% of the UK population use wearable tech

So of the two-thirds of the UK population who don't use wearables, it does not seem unreasonable to think somewhere less than a 1/3 of the two thirds might adopt wearables if privacy weren't an issue i.e. 22%. However, no trust solution will convince everyone, so we'll make the conservative assumption that a robust trust solution could boost adoption by 11%.

Above we've made some very rough ballpark estimates. The aim is to get a feel for the scale of the benefits that could be unlocked by the trust solution. Is it £1m, £100m, £1bn, £10's bn or more? Our estimates are summarised in the table below:

Opportunity	Opportunity size (£m's)	Value added by trust solution
Health Physical	£4,400	£484m
Health Mental	£28,000	£3,085
Social Care	£3,060	£336m
Insurance	£2,200	£240m

Figure 11: Summary of estimates

Looking at just the top four value opportunities, we estimate that the trust solution would underpin value opportunities amounting to ten's of billions and itself contribute **single figure £ billions of** value.

4.4 The changing market structure and who stands to benefit

Above we discussed how the creation of trusted flows of consumer Health and Wellbeing data, is creating a new market space sitting between the consumer and the providers of physical goods and services (see figure 7 above).

In this new space will emerge organisations that can build trusted data sharing relationships with consumers. This will enable these organisations to both provide digital-only services and also orchestrate the delivery of 3rd party services to the right consumers at the right time.

This new space may be filled by existing service providers extending their business models or by new entrant organisations. It is certainly a space of great interest and activity for the tech giants. So who stands to gain from this transformation? The answer to this depends to a significant degree on how the new trusted data sharing space emerges. This is also likely to shape the scale of the value created. We outline three scenarios:

- **Walled Garden: A single organisation orchestrates** the trust framework and also acts as a data facilitator for consumers' data. Such an organisation might offer a digital marketplace for consumer digital services and offer to integrate data and analysis with the providers of physical services. Organisations fulfilling this role could come from private or public sector, e.g. Google or the NHS.
- **Open: A coalition of stakeholder organisations orchestrates** the trust framework, while other businesses act as data facilitators for consumers' data. This separation creates an open ecosystem where a diversity of organisations can gain consent to access consumer's data and add value to their lives.
- **Open with a training dataset: A coalition of stakeholder organisations orchestrates** the trust framework, while other businesses act as data facilitators for consumers data. In addition, the trust framework coalition facilitates the creation of an anonymised training data set upon which new innovators can build new models and services. As above, but with consumers invited to altruistically or for-profit, donate their data to research and innovation within a framework that protects their identity and anonymity.
- In the first scenario, it is likely that due to commercial motivations or inertia the data sharing space will not be subject to the maximum pressure to innovate and evolve.

The consequence of this is a loss of potential value to the consumer and in all probability an excess (compared to fair market returns) of value retained by the organisation running the unified trust framework/data facilitator.

In the second scenario, the separation of the trust framework and the data facilitator role should ensure free access for innovative data facilitators. This in turn should increase the value returned to the consumer and create a fair value distribution between the facilitators and service providers.

The third scenario further improves the above by removing the barrier of innovators accessing training datasets to develop services to add value to the consumer.

5. Barriers to Growth

5. Barriers to Growth.
Key Takeaways

A number of barriers, inhibit the sharing of Health and Wellbeing data, which block the creation of value for consumers. In short, consumers don't trust businesses to use and share their data in the consumers best interests, while businesses are concerned about a consumer backlash if they get it wrong.

- 87% of consumers wouldn't forgive a brand for misusing their Health and Wellbeing data.
- Those consumers who were most concerned about privacy, were also the most prepared to share their data with a trusted 3rd party when they had transparency and control.
- Businesses consistently underestimate the consumer's willingness to share data with a party they trust.
- The inability of innovators to access training datasets in a safe, secure and trusted environment.
- 82% of Americans worried that smart devices would intrude upon their privacy. This was one of the top three reasons for not buying them.
- The main barriers to unlocking value from sharing health and wellbeing data are:

1. **Brand mistrust**
2. **Consumer's control of their data**
3. **Lack of transparency for the consumer**
4. **Complexity of data sharing for the consumer**
5. **Consumer access to 3rd party services**
6. **Fair value exchange for the consumer**
7. **Ability of innovators to access training datasets to create new services**

Most of these barriers result from consumer mistrust and can be overcome by creating rules and tools that make the data sharing transparent and controlled by the consumer. When consumers are given that transparency and control, they are more willing to share than businesses expect.

5. Barriers to Growth.

Several factors may impede the realisation of the value opportunities identified in the previous chapters. It is to these barriers that we now turn, to identify the barriers and explore what forces are creating them to arise.

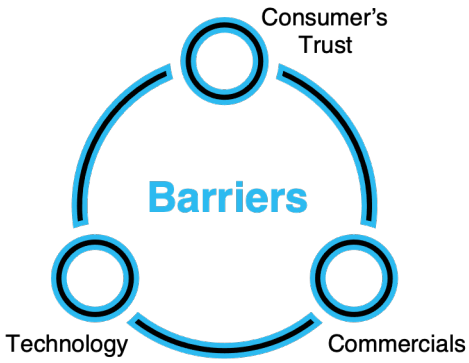


Figure 12: barriers to data sharing

5.1 Barriers to Data Sharing

Barriers to data sharing can be clustered into three broad groups: Trust, Technology and Commercials. Each of these can block or add friction to the data sharing process, leading to the value opportunity not being fully realised. This represents a loss of value to the consumer and is usually also a lost opportunity for the business that created the barrier.

Consumer Trust

Consumers mistrust organisations to use the data shared in the consumers best interests.

Consumers are often loathed to share their data for fear of the consequences of doing so. Essentially they don't trust, in some way, the organisation using the data. This mistrust can have a number of facets. It may be that it's not clear what they'll do with the data and for what purposes they'll use it. Or it might be that the consumer is wary of any more of their data being "out there" than strictly needed for fear it's hacked by a malign third party. Often the fears boil down to issues around transparency over the purposes for which their data will be used and the loss of control over that data.

However, when consumers' views expressed in surveys are unpacked, they are more nuanced than often reported. This oversimplification by many businesses leads them to be more cautious about data sharing than they need to be.

Technology

Complexity makes it hard for consumers to share their data, and organisations to understand it once received.

Technology can add friction to the data sharing process in a variety of ways. Digital Identity, authentication, a lack of API standardisation, data model ontologies, and consent mechanisms, can all make sharing data from one party to another and deriving value from doing so more difficult. Technology can present barriers both to 3rd party innovators creating services, and to consumers using those services. In both cases, the result is a loss of value to the consumer. Technology barriers can exist for a range of reasons from a lack of industry standards to deliberate attempts by a company to deter data sharing for commercial reasons.

Commercials

Commercial incentives can lead some organisations to put up barriers to consumers sharing data.

On occasions, commercial strategies may lead a company not to want to share data generated by their product or service. An example is when an early-stage company has ambitions to later build a service similar to those offered by 3rd parties. Or with late-stage companies who have large market shares and wish to exploit this through building a walled garden of third party services, that they can derive income by controlling admission to their ecosystem. Neither strategy is usually viable in the long run. The following explores each of these topics in more detail.

5.2 Consumer Trust

5.2.1 Anatomy of consumer mistrust

Consumer mistrust

According to a survey by TRUSTe (2020)[34], only 22% of consumers agreed with the statement "that the benefits of smart devices outweigh any privacy concerns." While PWC[33] found 82% of Americans worried that wearable devices would invade their privacy, which counted in the top 3 reasons for not buying a fitness band.

Further, many consumers mistrust consumer Health and Wellbeing device data for the management of chronic health conditions.

> *"Nearly 90% of those surveyed believe they could better manage chronic conditions with a health monitoring device. More than half of patients said they would potentially switch doctors if another doctor prescribed a specialized device……. while consumer-facing companies like Apple and Fitbit offer wearables with health tracking capabilities, only 28% of patients would trust a consumer device to help manage their chronic condition"*

Source Sony 2020

This concern is not entirely misplaced given data from consumer devices is not covered by HIPPA, the US health data protection laws. More generally a recent study published in the BMJ[30] found that 79 percent of health apps routinely shared user data but were far from transparent about the practice.

Causes of mistrust

Consumer's trust in how Health and Wellbeing businesses use and share their data is comprised of a number of distinct concerns (see figure 13) which can be distilled as:

- Transparency of purpose
- Respect for privacy
- No sharing without consent
- Clarity on terms and conditions
- More control over their data

The degree of consumer concern is also influenced by the scope of data being accessed. In general health and financial data are considered by consumers to be the most sensitive. This sets a high bar for Health and Wellbeing companies' data processing practices.

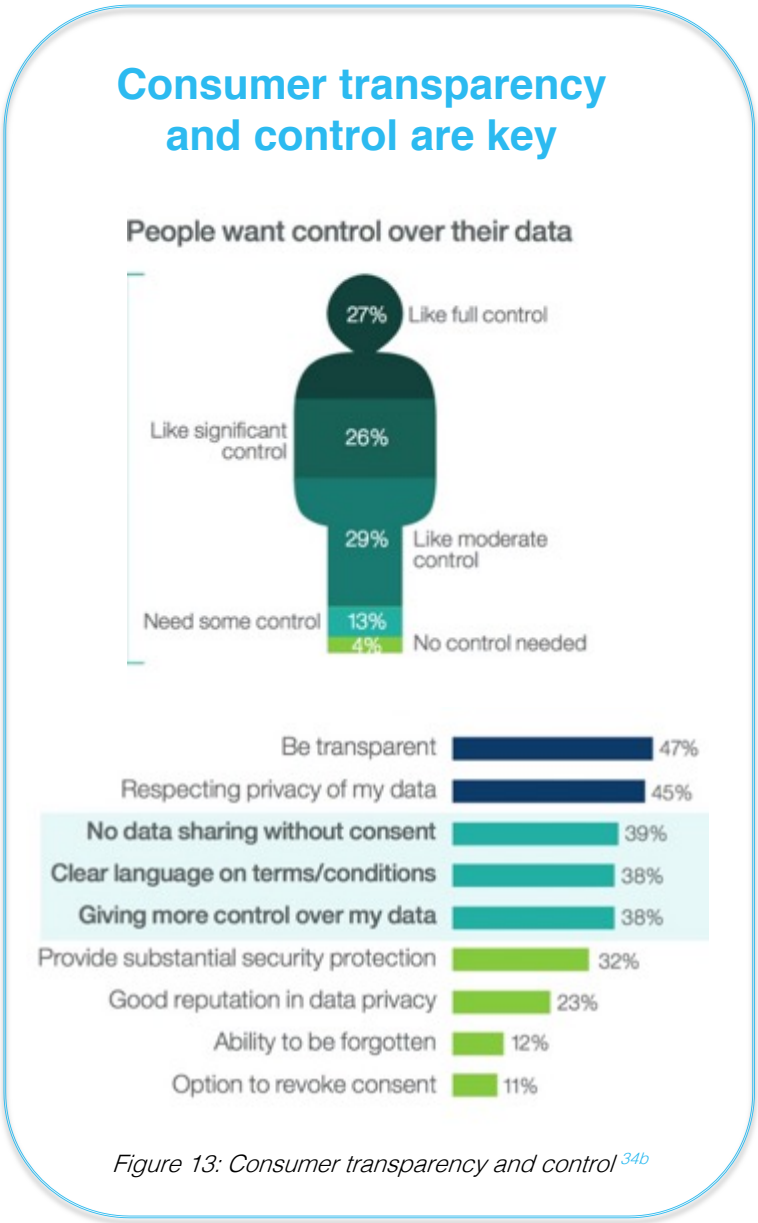


Figure 13: Consumer transparency and control [34b]

Trust as a brand differentiator

Consumer trust is a powerful commercial differentiator. A survey by Tealium[31] found that 97% of consumers were concerned about protecting their personal health data and 87% would not forgive a brand misusing their data, even if that brand were previously trusted. Being a trusted brand is a powerful commercial differentiator, with the research by Edelman 2020[32] finding:

> *"82% of US consumers say they will "continue to buy a brand they trust, even if another brand suddenly becomes hot and trendy." They also will pay more and continue buying a product from a trusted brand even if competitor reviews are better."*

30. https://healthitsecurity.com/news/majority-of-health-apps-share-user-data-without-transparency
31. https://tealium.com/blog/customer-centricity/as-wearable-health-devices-and-apps-increase-so-too-do-consumer-health-data-concerns/
32. https://www.marketingcharts.com/brand-related/brand-loyalty-109127
33. https://drugstorenews.com/news/pwc-future-wearable-tech-influence-healthcare-and-retail-delivery
34. https://www.prnewswire.com/news-releases/truste-internet-of-things-privacy-summit-is-the-first-event-to-address-the-privacy-needs-of-the-interconnected-world-264632091.html

34b. *Source: IBM Institute for Business Value 2017*

5.2.2 A new data sharing relationship

Data privacy vs sharing?

Inside many corporates, a discussion has probably occurred at one time or another, along the lines….

"Data sharing is a hot potato. There are a lot of privacy nuts out there who are maniacally opposed to it. If they target us, they'll damage our brand! Let's lock the data down!".

The problem with this narrative is that consumer surveys show it to be generally untrue and such views are causing companies to behave in ways that miss opportunities to create value for themselves and their customers. Work published in the Harvard Business Review[35] ("Do You Care About Privacy as Much as Your Customers Do?", 2020) shows that the 32% of the population who most actively switch brands in response to privacy breaches are also the group that's most willing to share their data if there is the right degree of transparency, control and value exchange (see figure 14). Those concerned about privacy, are the most willing to share their data under the right conditions:

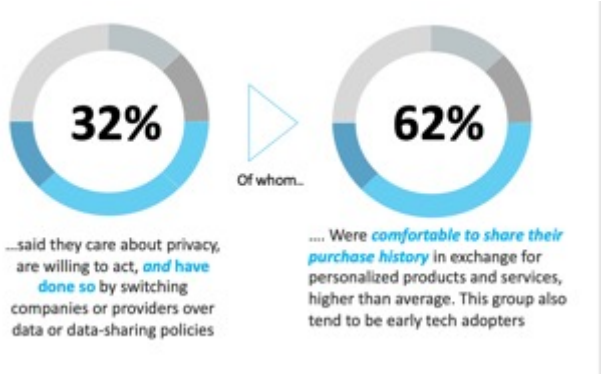


Figure 14: Consumer views on privacy vs data sharing

Those concerned about privacy aren't the laggards, they're the early adaptors, the well educated and technically savvy, who are demanding business on their own terms. It may be that they are giving companies a glimpse of the future, not the past and it could be rash of businesses not to effectively engage with their needs.

Business fears

More broadly, companies who properly engage consumers, appear needlessly conservative about limiting the purposes for which they use customer data. BCG research in 2015[36] shows that when properly engaged consumers are more happy to share than businesses expect (see figure 15).

Businesses underestimate consumers willingness to share data

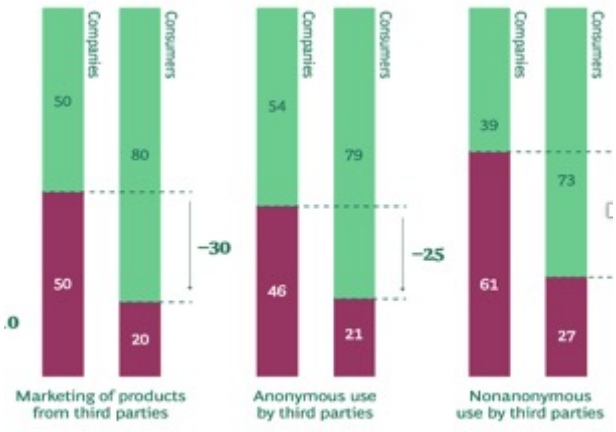


Figure 15: Consumer vs business views on the acceptability of data sharing (source: BCG Data Misuse report)

The keywords here are "properly engaged". Any brand wishing to motivate the customers to share data needs to address trust, complexity and fair value exchange. Brands might like to ask themselves:

- **Brand Trust:** Have you built that trust with consumers giving them transparency and control over their data?
- **Fair value exchange/commercials:** have you articulated a fair and compelling value exchange in return for the data?
- **Complexity / Technology:** Do you make it simple for your customers to share their data?

When these tests can be answered positively, the research suggests that consumers embrace sharing their data. In doing so they build trusted durable relationships with the brands that engage and serve them properly.

The concerns of businesses are intensified by the fact that at the moment they feel like they are in control and are 100% responsible for the relationship with the consumer. With the new well-documented consumer need for more control and transparency, the division of responsibility of this relationship needs to be redrawn. A new data-sharing relationship is needed at its heart, enabling new approaches to customer journeys, service models, costs and risk management.

Work by McKinsey et al (2019)[37] demonstrates businesses that are relatively more competent with data and analytics are outperforming their competitors. However, this is often seen through the lens of technology and staff training. Increasingly important will be how businesses "properly engage" their customers to build trust and earn the right to access and use that data.

35. https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do?registration=success
36. http://media-publications.bcg.com/23nov2016-survey.pdf
37. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/catch-them-if-you-can-how-leaders-in-data-and-analytics-have-pulled-ahead

5.3 Complexity and Technology barriers

In what follows we will explore the barriers of complexity and technology barriers that inhibit consumers sharing their Health and Wellbeing data.

5.3.1 Privacy communications

Research by Deloitte's in 2019[38] suggested that 82% of consumers have taken action in response to their privacy concerns over the last year, the same percentage (81%) who say they never read terms and conditions". T&C's are an ineffective way of engaging consumers.

An alternative approach has been developed by "DataSwift" and others, to create a standardised iconography to communicate the purpose the data is being requested for and aspects of how the data will be processed. These are analogous to food content labels commonly used by supermarkets.

To date these data labels have not been widely adopted but may represent a better route to more effectively communicate and engage consumers about privacy issues.

5.3.2 Technical Standards

Another barrier to data sharing arises from a diversity of standards or standards not being implemented for the data ontology. This makes the data complex to interpret for the 3rd party service providers. In the field of Health and Wellbeing data, this issue has been greatly reduced by the widespread adoption of OWL/FHIR. Indeed healthcare-related fields probably have more mature data ontologies than most other sectors.

Another challenge can be connecting 3rd party services to the API of the service providing the data. Ideally, these APIs are well defined and open APIs, but service providers may choose to restrict access to them.

5.3.3 Consent Architecture

To enable the consumer to control the sharing of their data, a consent architecture is needed, that:

- Makes it easy to give or refuse consent
- Makes it easy to see what consents are in force
- And then revoke those consents when desired.

Ideally, the consent architecture will enable "consent requests" to be embedded into the service flow e.g., via a pop-up window, so that consumer's aren't handed over to separate parts of the service to grant consent. Some form of dashboard is also needed for consumers to view the consents that they have given and offer the functionality to revoke them if they wish. In addition, there needs to be some common definitions of the words used in the consent requests. For instance, it would be confusing for the consumer if two different 3rd party services defined the scope of activities implied by the word "Advertising" differently.

Solutions to these problems have been developed by a number of "Data Intermediaries" e.g.Meeco, Digi.me, Polypoly, DataSwift. These capabilities can be embedded within a service and manifest as the consumer's "data account". These "accounts" then give consumers the tools to manage those consents. Another advantage offered by Data Facilitators is that when a consumer wishes to share data from many sources to many services, they reduce the number of consents a consumer needs to give (see figure 16), reducing the burden for consumers and business benefits and enabling value to flow, as shown below:

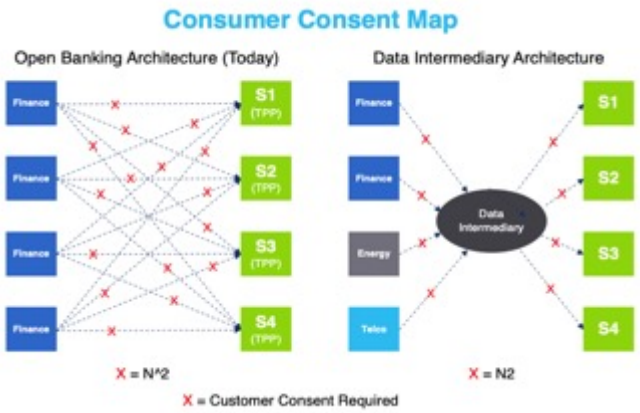


Figure 16: How Intermediaries reduce the consumer burden of the number of consent requests

5.3.4 Service creation

A final technology barrier may be the availability of sample data which 3rd party innovators can use to train their models. Without such training data, it may be difficult for innovators to understand the power of the Health and Wellbeing data and incorporate it into the 3rd party services which they are creating.

38. https://www2.deloitte.com/uk/en/pages/press-releases/articles/dicing-with-data-proportion-of-consumers-very-concerned-over-sharing-data-online-halves-in-two-years.html

5.4 Commercial Barriers

Consumers want businesses and markets to offer fair exchanges of value and maximise their opportunities for value creation. This section explores these commercial barriers faced by consumers.

5.4.1 Fair value exchanges

A survey by Orange has found that only 6 per cent of respondents felt consumers benefit the most from data sharing, while 67 per cent believe it is companies that benefit. A similar result was found by the Digital Catapult[39] in 2015, which surveyed 4,005 people of whom nearly 80% said data sharing was primarily for the benefit of business rather than the consumer.

Consumers' perception of a fair value exchange depends both on what the data is and the purpose for which it is being used. Research by Timothy Morey et al (2015), see figure 17, illustrates the heatmap of consumer value expectations as a grid of data vs use.

Figure 17: How consumers perceive "data value"

Overall, consumers attribute a high monetary value to their data. In a survey by Curtis[40] (2016) the average UK consumer would ask for £3,241 if they were to sell all their personal data. Specific services require rather less than this quantity of data and so more modest value exchanges are needed. The critical thing is to make the value exchange clear and explicit at the point the consent is requested.

The nature of the value exchange is proposition dependent, and often best structured incrementally with specific requests occurring at the point in time that the consumer wants to use that part of the services which relies on the requested data.

5.4.2 Impact of Market Structure

Another type of commercial barrier can arise from the market structure. This can arise in at least two different forms.

Firstly, if a competitor has achieved a bigger market share than it's competitors, then one competitive strategy could be to leverage their scale to build a walled garden of 3rd party services. Such scale effects, handled correctly, can accelerate the growth of their ecosystem, attracting evermore 3rd party services. At its core, such an ecosystem facilitates data sharing between the core platform and the 3rd party services and typically inhibits sharing beyond the walled garden. This is a double-edged sword from the consumer's perspective since the diversity of 3rd party services might only be available via one particular core service/device. This may result in a form of lock-in which persists even if in the future the quality of the core service/device falls behind that of competitors.

The second flavour of this lock-in occurs when a Health and Wellbeing digital service is acquired or merged with another business from a neighbouring market, enabling synergies. This enables the business to use those synergies to differentiate their products and they may seek to preserve that differentiation by impeding data sharing with competitor services who lack their own footprint in both markets. Again the net result is a double-edged sword for consumers, who gain short-term benefits from the synergies created but suffer a long-term loss of value from reduced innovation and less effective competition.

Neither of these commercial barriers are inevitable. Companies in the situation described above may choose to embrace a genuinely open ecosystem approach for a variety of good reasons. However, given recent M&A activities in the Health and Wellbeing market, these risks may become relevant in time.

39. https://www.computerweekly.com/news/4500250709/UK-consumers-do-not-trust-organisations-with-data-says-survey
40. **The value of our personal data in the Big Data and the Internet of all Things Era by Anahiby Becerril**

5.5 Summary of Barriers

Through this section, we have looked at the challenges which today inhibit the creation of value from consumer Health and Wellbeing data. We can summarise the barriers as:

1. **Brand mistrust**
2. **Consumer's control of their data**
3. **Lack of transparency for the consumer**
4. **Complexity of data sharing for the consumer**
5. **Consumer access to 3rd party services**
6. **Fair value exchange for the consumer**
7. **Ability of innovators to access training datasets to create new services**

For reference we will recap each of these in turn.

5.5.1 Brand Mistrust

Trust in a Health and Wellbeing service brand significantly determines whether consumers are willing to share data with that brand. Trust in the brand underpins consumers belief that the claims and promises made, about the purpose of the sharing, transparency and control, are true. Today, the sharing of Health and Wellbeing data does not have a widely accepted trust brand or "Trust Seal", making it hard for consumers to know which claims to trust. The resulting mistrust leads to consumers being reticent to share their data.

5.5.2 Consumers' control of their data

Consumers want control over what data they share and the ability to be able to stop sharing it when they want. Often services bundle multiple consents into one step on the consumer journey and offer no easy tools to then subsequently manage those consents. The perceived loss of control over their data leads consumers to minimise the data they consent to share in the first place.

5.5.3 Lack of transparency for the consumer

Consumers often find it hard to comprehend what data sharing consent is requesting. The language used is often complex and frequently "loaded" to nudge them toward consent or opaque, leading them to suspect that it contains "sneaky stuff". To limit the risk of them consenting to the unknown they decline to share their data.

5.5.4 Complexity data sharing for the consumer

If a consumer wishes to share their data, the complexity of the process to do so can act as a barrier in itself. Often they have to log into a 3rd party service provider, navigate a series of warning notices and then may have to repeat the process periodically. This poor user experience is another type of barrier to data sharing.

5.5.5 Consumer access to 3rd party services

Some providers of Health and Wellbeing services or devices choose to limit consumers ability to share their data with 3rd party services. Typically this is for reasons of commercial strategy if they themselves want to provide services similar to those 3rd party services. This may act as a barrier to the creation of value for consumers.

5.5.6 Fair value exchange for the consumer

Some consumers are deterred from sharing their data because they feel that the value created by that service provider is inequitably shared with the consumer. Typically this arises where a service provider feels advertising is an inherent feature of their service, whereas the consumers are happy that their data is used for the service's purpose but not for advertising. This leads some consumers to not want to share their data with services that they believe will "sell" their privacy. The concept of fairness and privacy are deeply intertwined.

5.5.7 Ability of innovators to access training data to create 3rd party services

To create new services that deliver value to consumers, innovators often need access to data to create the machine learning models that underpin many of those services. Presently, there are few Health and Wellbeing anonymised data sets upon which they can build such models. Access to data is acting as a barrier to market entry for those able and willing to create value for the consumer.

6. Solution Framework

6. Solution Framework.
Key Takeaways

In this section, we propose a solution hypothesis to help overcome the barriers to consumers sharing their Health and Wellbeing data. Many of the components needed already exist, although some gaps remain.

- A holistic “consumer trust solution” spans governance, liability models, standards, technology, user experience patterns, data labelling and trust seals.
- Many of these components exist in some form, to some level of maturity, in the market today. The biggest gap is around a recognisable trust label and standardised data labels.
- From consumers’ perspective a holistic market trusted data sharing solution manifests as a quick and easy way to understand and trust that their data is going to be treated fairly. E.g., Trust Labels (ensuring transparency, communicating ethics), consumer tools to manage their consent to data sharing, consumer tools to manage their personal data.
- To deliver the holistic solution requires collaboration between an ecosystem of stakeholders as many of the components require different types of organisation to deliver them e.g., a Trust Seal requires a consumer trust solution, data sharing safety and security standards requires standards and governance, Trusted UX Patterns requires consumer brands.
- A phased solution, creates an easy entry point for stakeholders. The “Solution Hypothesis” developed herein enables an evolution towards a holistic solution with 3 main phases:
    - Phase 1: Trust seal and data labels
    - Phase 2: Consent tools
    - Phase 3: Data management tools
- Each phase requires a distinct set of components across a set of stakeholders

As the governance, infrastructure and standards mature, the consumer-facing features, such as the data labels, are progressively enriched easing the burden on the consumer to gain control and transparency over the use of their data. This in turn enables the greater use of the data and increased value to flow.

The presence of a Data Trust Label in the market unlocks the value from the other market components (which are generally more mature), in turn unlocking value in the market for all stakeholders.

A Data Trust Label for consumers empowers the consumer to have a voice and hold collective power by making informed decisions.

6. Solution Framework.

To overcome the barriers and gain access to the value opportunities that the use of Health and Wellbeing personal data offers, requires a number of market components to be facilitated and orchestrated. Together, maturing over time, these components enable a consumer trust solution that supports the development of a vibrant, valuable and open data sharing ecosystem.

6.1 Solution Hypothesis

Drawing on:

- A review of what's already in the market
- Two stakeholder expert workshops
- Over a dozen expert interviews
- Ctrl-Shift's work over the last 11 years

A catalogue of market components was developed that were able to contribute toward building a consumer trust solution for Health and Wellbeing data sharing.

6.1.1 Component Interaction

To enable us to understand the interaction between these components, they can be grouped into six 'component clusters', three being visible to the consumer, what we call "above the line", and three being invisible to the consumer, what we call "below the line", but enable the 'above the line' components to function. It's only when these above and below the line components are combined that the market will function effectively (see figure 18).

It is perhaps easiest to use a comparison of this structure with the electricity market, where the "above the line" components are washing machines, hoovers and light bulbs which make electricity valuable and safe for us all to use in our everyday lives. And we know they will work and are safe because of the "below the line" components of power stations, pylons and sub stations that deliver the electricity to a standard that is governed and makes electricity easy and safe to use.

In the electricity market, one can debate whether fuse boxes are above or below the line, they are the intersection between the electricity infrastructure and the electricity use. Whichever they are they are essential components in the overall market. In the personal data sharing market the debate about the intersection between the above and below the line is similar and unless progressed, runs the risk of stalling the development of the market impacting the value creation for individuals, society and the economy and leaves existing risks in the market to continue unchecked.

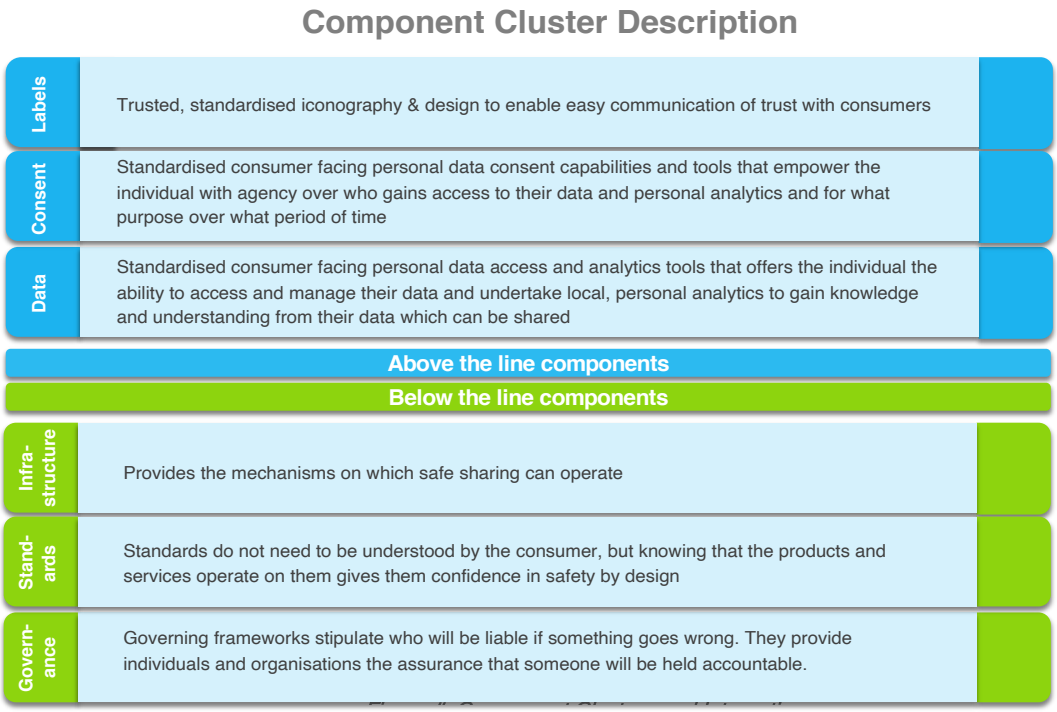


Figure 18 Component Clusters and interaction

6.1.2 Multi-Functional Stakeholders

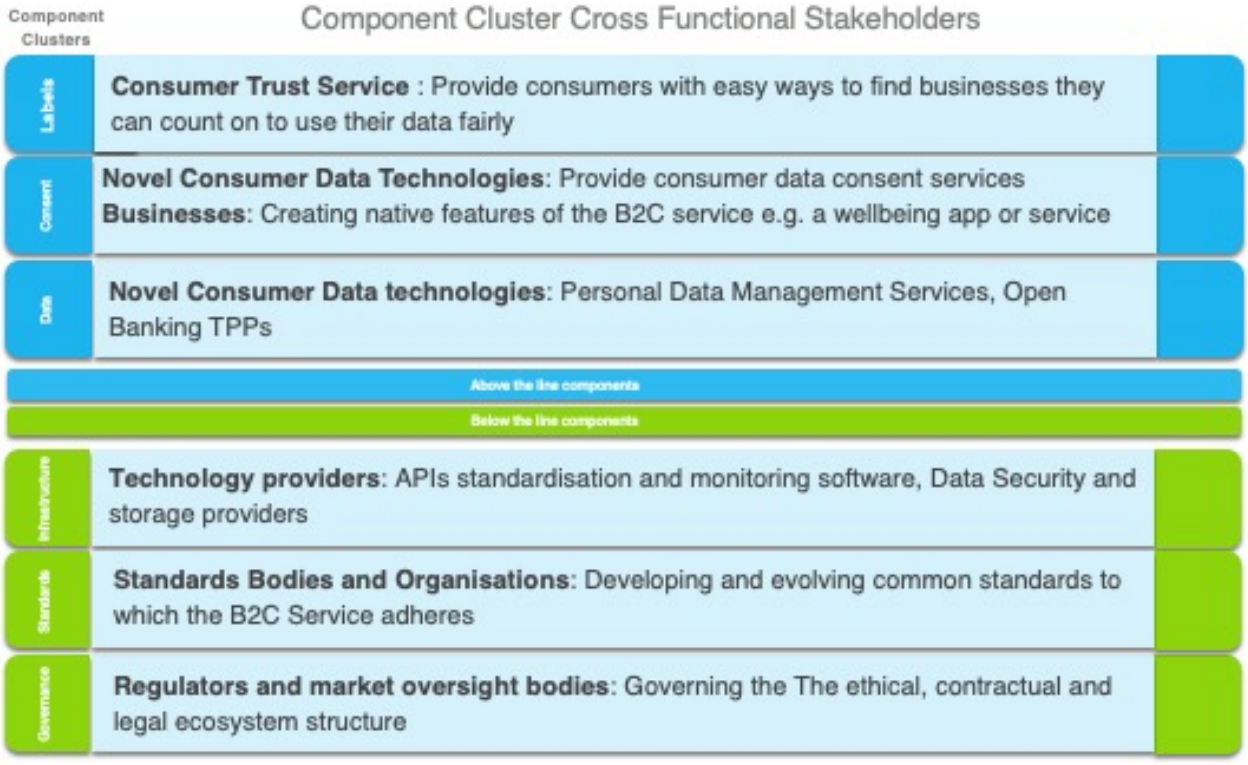


Figure 19 Component Clusters Multi-Functional Stakeholders

As we examine these Component Clusters we also see that the delivery of each falls across a multi-functional set of stakeholders, most notably:

- **Consumer Trust Solution**, which ensures the consumer gets fair value and remains safe.
- **Novel consumer Technology providers**, equipping the consumer with digital data tools.
- **Technology infrastructure** providers.
- **Standards bodies** and entities.
- **Governance** oversight, either official or self-governed.
- **Innovators,** both incumbents and entrepreneurs, who design and deliver the services that create the value for the individual.

Figure 19 above illustrates which component clusters these types of players support. It is the need for the orchestration within and between the layers of Component clusters, and the need for multi-functional teams to develop them, that calls for facilitation and orchestration of the development of the market, in which even large and multi-functional players such as Pharmaceutical companies or Telecoms providers can not overcome the barriers to value creation alone.

Returning to the example of electricity where early value was created through the electrification of large conurbations, Wabash, Indiana became the first electrically lighted city in the world in 1880, in the digital data-driven economy value can be created within Ecosystems that are focused on specific value opportunities and with a closed group of stakeholders.

This is already happening within Walled Gardens such as Apple's App Store, however, if we are to see the benefits at scale for individuals, our societies and our economies the design needs to be scalable beyond the Walled Gardens, not used to create barriers to entry.

6.1.3 Above the line components and maturity

Timing is everything and understanding the maturity of the components already in the market provides an indicator as to when the time is right to begin to design a scalable market solution for trusted personal data sharing. For this reason, we have estimated the maturity of the components, critically are they available somewhere in the market today?

To be clear, by maturity we mean how adequate are the capabilities that exist today, rather than implying at what scale they are used today or their use in the Health and Wellbeing market. By way of an example, the Trusted Third Party Providers in the Open Banking market provide a personal data management service functionality for bank data sharing, they have at scale technology and business models, however, they have not yet been applied in the Health and Wellbeing market. A rough assessment of the different component's maturity is presented in Figure 20 (below) for the line components.

It's also noteworthy that although there exists some level of maturity across the Labels Cluster, there is no or very limited maturity in the Trust Logo's Kitemarks and Ratings components, which indicates to the consumer trusted data sharing market actors or services. However, a number of supporting components are at varying levels of maturity.

This suggests that Labelling is the most immature part of the trusted data sharing market, while other supporting components such as consent and to lesser degree data management are rather more mature.

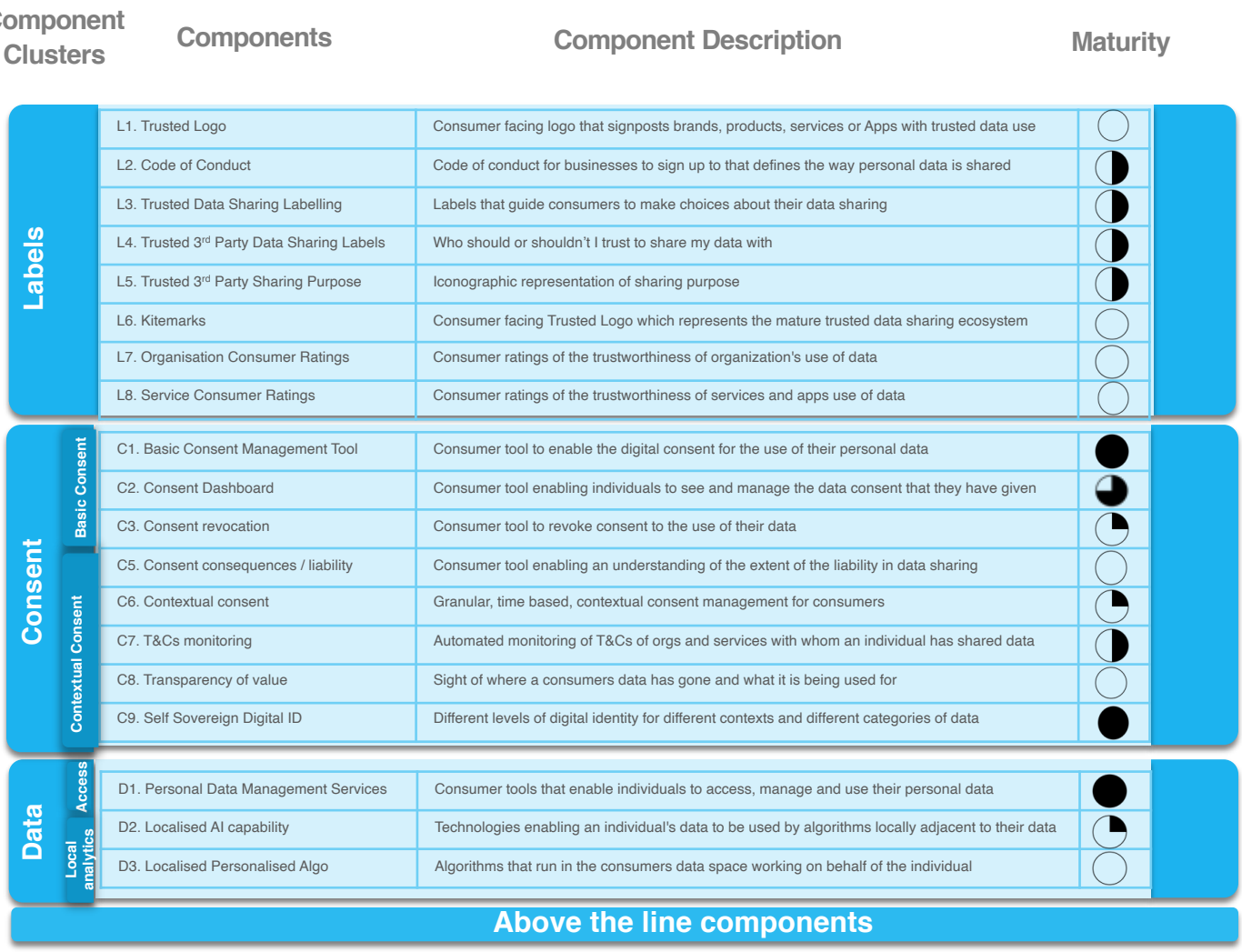


Figure 20: Above the Line Component Descriptions and Maturity

This analysis suggests that maturity levels are mixed across the component clusters, however, that there are a number of components that are at a reasonable level of maturity.

These may together enable early-stage development of trusted data sharing, see the later section in this document on the potential phases of market development.

However before concluding that the time is right for the development of a sustainable Trust Label, an understanding is needed of the impact each component cluster has on the barriers to value creation, the maturity of the below the line components and how different components may be orchestrated to achieve a trustworthy solution.

6.1.4 Components Addressing Barriers

To understand the importance of each of the component clusters to the overall trust solution we need to analyse the degree to which each Component Cluster overcomes the barriers to value creation identified in section 5, for both consumer and business. This enables us to understand which makes a strong contribution to the development of a trusted personal data sharing market, and in so doing enable access to market value.

In section 5 we identified a number of barriers to trust personal data sharing and broader value creation from sharing Health and Wellbeing data. To recap these barriers were:

Barriers to value creation:

- **Trust anchor:** a brand or organisation that consumers trust to oversee their data sharing.
- **Consumer control of their data:** giving consumers ongoing control over what data they share.
- **Fair exchange of value:** to be clear about what value consumers will receive for sharing each attribute of data.
- **Ability to create 3rd party services:** The ability for innovators to access data sets to create new services

We can now estimate to what degree each of our component clusters addresses each of these barriers. This is shown in the table below (figure 21).

By exploring the Component clusters ability to overcome the value barriers, we see a number of insights emerge. Firstly, none of the Component Clusters can adequately address all the barriers. Rather, each contributes their own, often unique value.

It's only by combining most of the Component Clusters that we can see a holistic solution emerge. Even then, one of the value barriers, that of ensuring "a fair value exchange", is only helped, but not solved using these components.

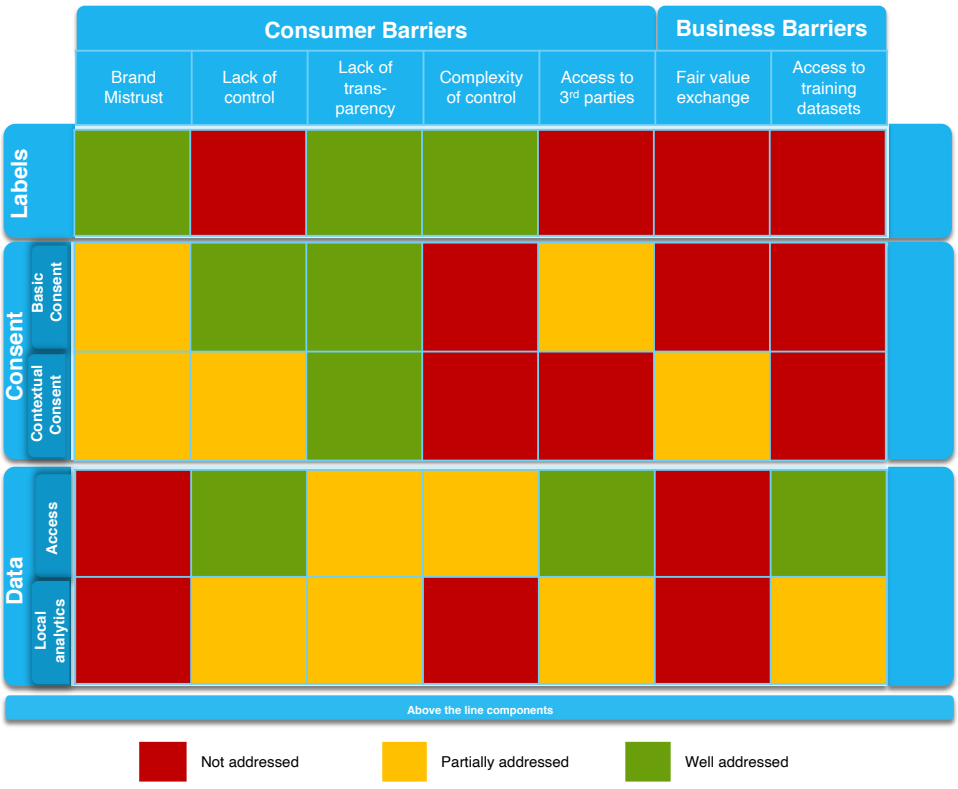


Figure 21 Component Clusters overcoming Barriers

- **Transparency for the consumer:** A simple way to communicate what is shared, with whom, for what purpose, for how long and what are the risks.
- **Complexity for the consumer:** to make the process of sharing data on an informed and consented basis simple.
- **Access to 3rd party services:** to share their data with 3rd party providers of their choice

We hypothesise that Fair Value Exchange can be enabled by leveraging all the Component Clusters to build services and business models that reflect principles of fairness. This offers an opportunity for businesses to not only create unique value, but also to build brand trust with the consumer increasing their loyalty and reducing churn.

6.1.5 Below the line components and maturity

The 'Below the Line' components are normally unseen by consumers and serve to enable the 'Above the Line' components, the level of maturity of these components will determine the degree to which the consumer or the business has to bear the cost and risk.

Example 3: Without mature 3rd party validation the consumer has to risk not knowing whether the organisation or person they are sharing their data with is authentic or trustworthy, businesses are unable to dynamically share data across supply chains limiting the value they can create and increasing the burden of business in participating in digital supply chains.

Figure 22: Below the line components and maturity

Many of the Below the Line components are moderately if not fully mature, often coming from other sectors or different markets.

Example 1: the World Economic Code of Conduct for Personal Data Sharing is for international use and can be built on to support nuances in specific regions, countries and sectors.

Example 2: API design and monitoring technology companies designed for the finance sector are strategically developing horizontally across sectors.

The level of maturity of the Below the Line components leads to a conclusion that alignment and orchestration of these components are likely to be able to support the development of Above the Line components and so accelerate access to the value.

While the component maturity table gives us a feel for the range of components that we can potentially draw on to create a solution, we note that many of the components can't meaningfully be deployed in isolation. There are heavy interdependencies between them. For instance, trust seals and data labels are next to useless without adequate governance structures.

6.1.6 Phased value access

Because of the interdependencies between the layers, we need to identify vertical cuts through the components, linking together components above and below the line that together can be combined to make a meaningful and coherent difference to consumers. We've identified 5 vertical cuts (figure 23).

Viewed this way, while a holistic solution to consumer mistrust is a complex beast, it is deployable in bite-sized pieces, each component of which adds value in its own distinct way.

Our hypothesis for a consumer trust solution could consist of a number of distinct phases:

Phase descriptions

Phase 1: Single Service Solution: Supporting the trusted use of data within single services supported by standardised Trust Labels with a Code of Conduct.

Phase 2: Closed Ecosystem: Trust built within an ecosystem confined to a predefined set of players with a tightly walled garden to ensure that trust is maintained. As above, but with a consent dashboard that spans services, governed data sharing labels within each consumer app/service.

Phase 3: Open Ecosystem: Trust enabled across an open ecosystem leveraging the closed ecosystem components but with tools for consumers to aggregate data and run algorithms locally/privately.

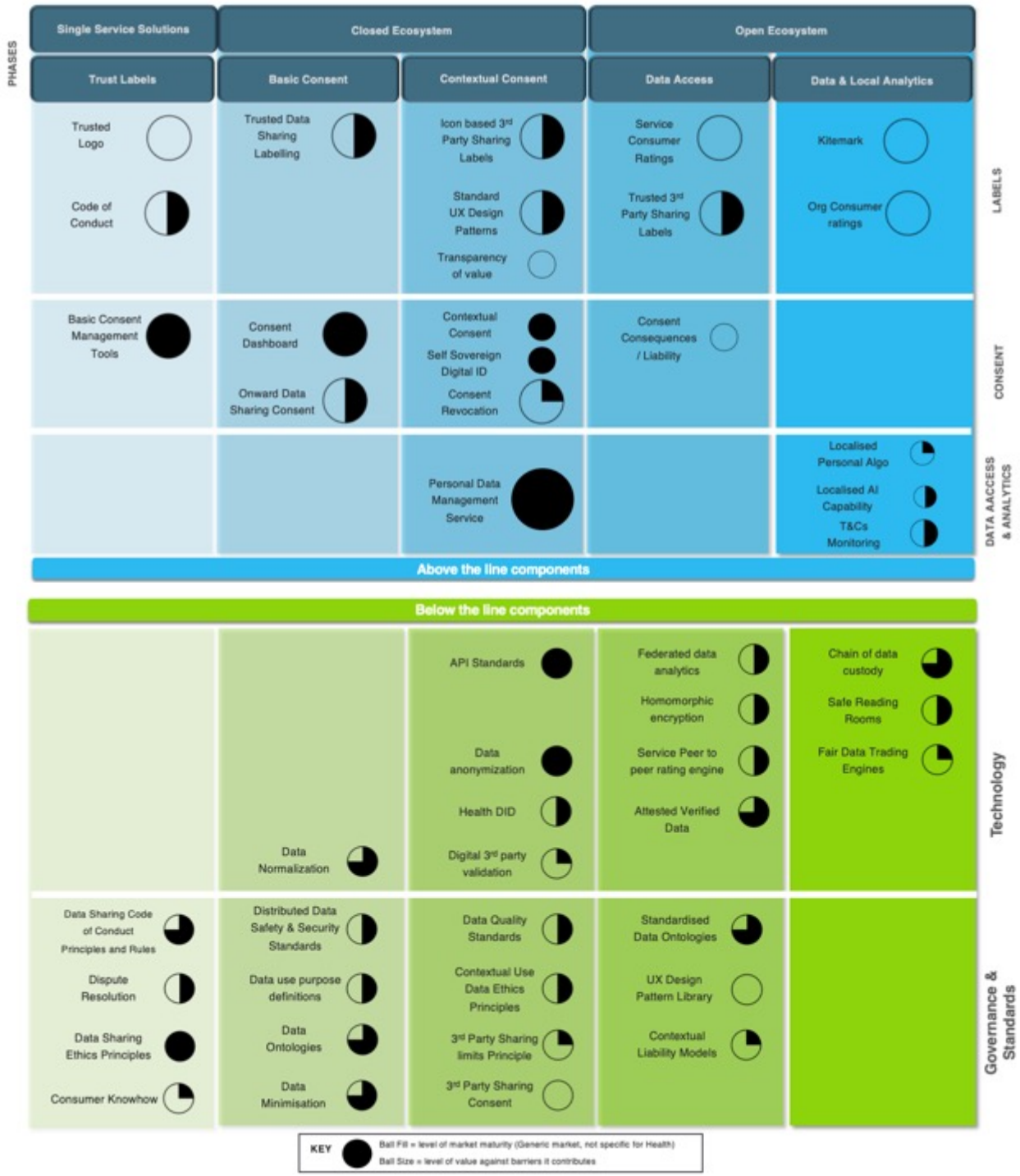


Figure 23: Above the Line Component Descriptions and Maturity

6.2 Phasing of the Solution Hypothesis

From this analysis, it's clear that trust labelling, in the form of widely recognised trust marks or data labelling, is a significant gap in the market. With no widespread standardised labelling, it's hard for the consent and data components to gain traction. This suggests if the labelling problem were solved, it could unlock other already mature components to bear down on the challenge of building consumer trust in sharing their Health and Wellbeing data and enable access to significant additional value for consumers, society and businesses.

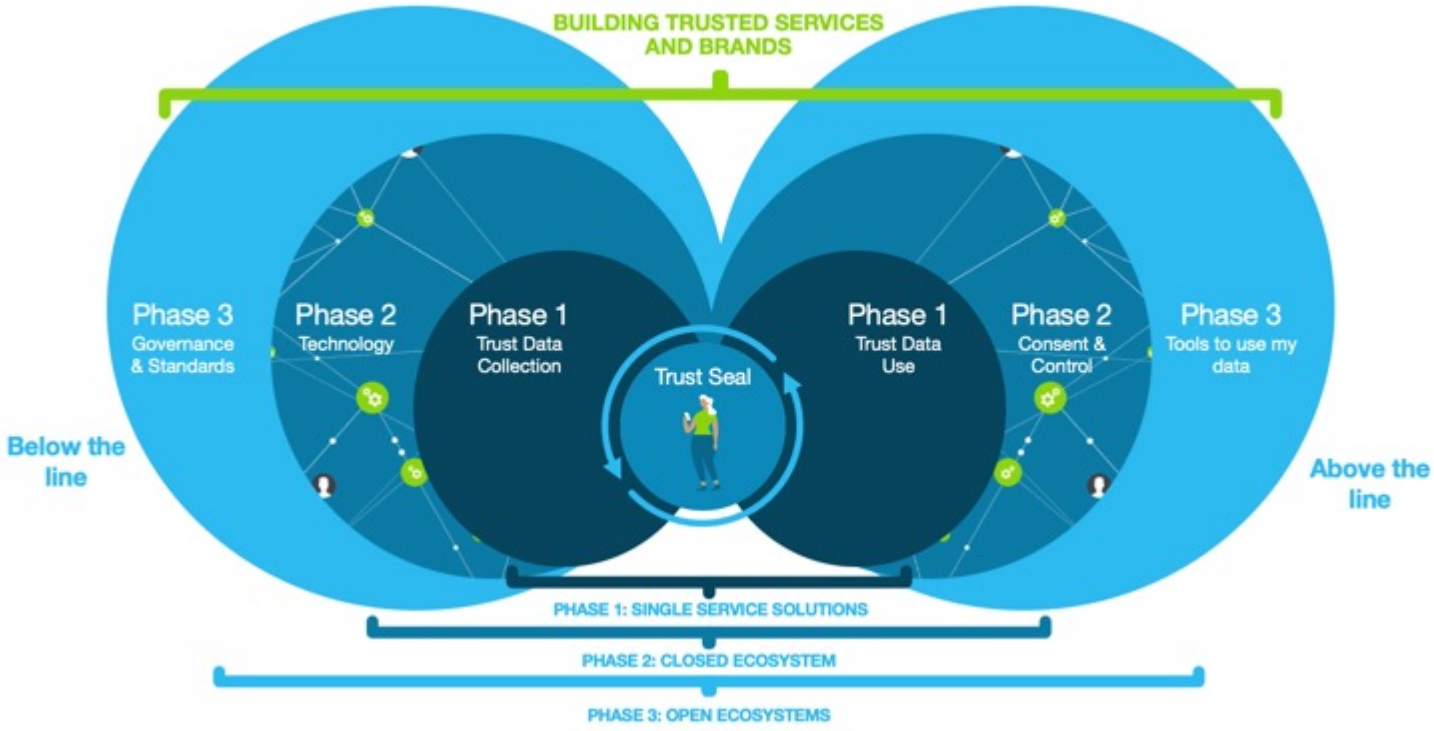


Figure 24: Three phases of development

More generally, we see "labels" such as trust seals and data labels (Phase 1) as helping overcome the trust and complexity barriers for consumers and businesses. Consent (Phase 2) in turn strengthens the labels while adding consumer control.

As we move on to also put data and analytics in the hands of the consumers (Phase 3), we see this further strengthens their control of their data and increases their ability to autonomously interact with 3rd party services in a safe, privacy-preserving way.

The hypothesis for a holistic trust solution outlined above, in figure 24, is not the only conceivable scope or evolution. It does, however, represent an attempt to marshal the components that we have identified in a structured way, to overcome the barriers to consumer trust and value creation.

The phases are reasonably intuitive, with a simple starting point and building complexity over time, with each phase offering consumers and businesses distinctive value.

The following describes the phases and the successive value created for each.

Phase functionality and value

Phase 1 Single Service Solutions

Functional Description: The code of conduct has two facets, 1) a short, simple, easily understood set of principles for consumers to read. 2) richer rule set codifying what behaviours are mandated for organisations. Organisations satisfying the schemes governance body that they comply with the code are entitled to display a Trust Seal. Consumers who feel an organisation has breached the code can take their complaint to the governance body who will operate some form of dispute resolution process.

Benefits for consumers: Simplified ways to identify trustworthy organisations and confidence in a course of redress through a neutral process.

Benefits for Businesses: The opportunity to differentiate themselves through ethical conduct visible to consumers.

Closest examples today: Truste, TrustArc, MSC, WEF Personal Data Sharing Code of Conduct

Phase 2 Closed Ecosystem

Functional Description: As phase 1, with the addition of a standardised consent infrastructure. Consents are requested in a layered/incremental way, with only the data actually needed for the current point in the user journey being requested at that point. Each consent request is in a standardised format that uses iconography to communicate what data is being requested, for what purpose, by whom, for how long and other contextual risk information. All consents given are visible in the consumer's single consent dashboard operating across all their service providers who are members of the scheme. The dashboard gives the consumer the ability to revoke their consents at any time.

Benefits for Consumers: Transparency as to what the consent requests actually mean. A fairer value exchange underpinned by granular consent requests being presented close in time to the value derived from sharing their data being received by the consumer. Effective control over their data sharing through the cross-service provider consent dashboard.

Benefits for Businesses: Future proof their compliance process. A tangible demonstration that they respect the customer's wishes and are not doing "sneaky stuff". Access to more data sources by building customer trust.

Closest examples today: Forgerock, Apple AppStore, iubenda, OneTrust

Phase 3 Open Ecosystem

Functional Description: As phase 2 with the addition of a standardised infrastructure enabling the consumer to aggregate and control the analysis of their data. The consumer has a private data space (e.g. personal data store) in which they can privately aggregate their data and run 3rd party algorithms on it.

This gives them the choice to share access to either the raw data or just the results of those algorithms as insights. In addition, they have the option to draw on a range of privacy-enhancing technologies to share their data in a modified form (differential privacy, homomorphic encryption etc.) to gain utility while protecting their privacy.

Benefits for consumers: The ability to largely break the linkage between sharing their data and compromising their privacy. Access to a broad ecosystem of businesses that provide new value in their lives.

Benefits for Businesses: The ability to adopt new paradigms of being businesses driven by personal data, without actually holding or touching that data. This greatly assists their compliance and reduces their data risks and liabilities. Further, it enables them to significantly differentiate their offering to consumers and build deeper, trusted consumer relationships.

The trusted flow of data opens up opportunities for the design of dynamic digital supply chains that use the data to configure solutions that create value. With digital data oversight, the opportunity to digitally monitor compliance offers reduced risk and cost opportunities.

The ability to support a dynamic ecosystem of innovative businesses that can be easily assessed for risk and compliance. Low entry costs for innovative businesses creates an opportunity for a vibrant digital ecosystem that supports an uplift of trust and value.

7. Design Considerations

Design considerations for a Consumer Trust Solution

7. Design Considerations.
Key Takeaways

The Design Considerations offers a more detailed view of the existing market solutions across the Component Clusters. Examining these supports the more detailed design work to carry out further development work to enable consumer generated data to be used outside a clinical setting to support the consumers Health and Wellbeing. This deeper analysis exposes some clear design considerations:

There is a clear link between the Trust Labels and the Governance structures

There are a number of emerging Personal Data Sharing Governance Structures which have common characteristics:

- The Individual's Control
- The Individual's Transparency
- The Individual's Privacy
- The fairness in value exchange
- All actors accountable

Many of the available Consent, Data and Infrastructure components have developed proprietary Governance, quasi-Standards which rely on their brand to provide the market Label function on which the consumer needs to trust. Working with one or more of these would provide valuable insight to support iterative testing within the Health and Wellbeing setting.

A number of Standards are already in market, although many are outside the Health and Wellbeing setting it is likely that many can be repurposed.

Similarly, a number of common technology components such as API platforms, security and storage providers are already in play in other markets and actively seeking cross sectoral market opportunities.

Close working with one or a number of Governance organization's when designing a Labels solution would enable rapid progress.

An essential founding for a market solution is a set of Ethics Principles which provide the boundary for the Governance structures and therefore the Label.

7. Design Considerations.

In this section we will look at the design choices needed for each of the components clusters identified in our solution hypothesis in section 6, and described in the table below:

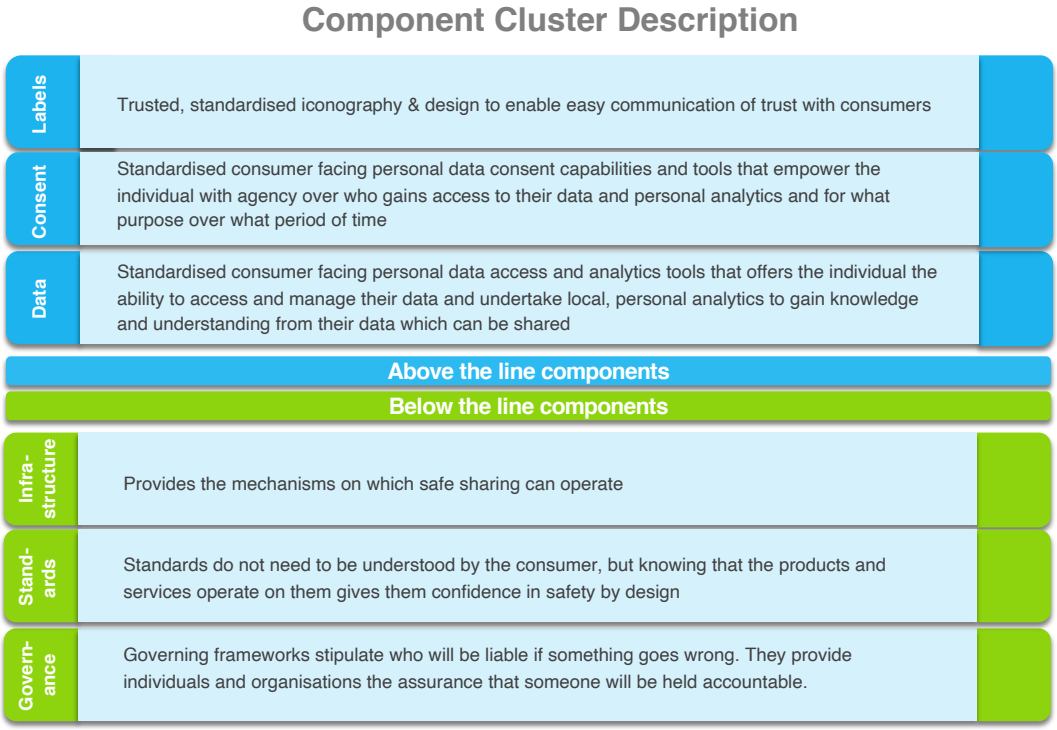


Figure 25: Description of Component Clusters developed in Section 6

In these considerations, we intend to suggest a direction of travel for the more detailed design work to be carried out in the 2nd Phase of this project.

By examining in more detail some of the exemplar solutions across the Component Clusters (Clusters), we are able to understand if there are commonalities that provide guidance for the future market solutions, if there is anything existing in market that would or could be repurposed or if there are particular components that would enable strong progress, enabling the consumer generated data to be used, outside a clinical setting that supports their Health and Wellbeing.

The choices made across the Clusters also have a big influence on the pace at which the value can be accessed by consumers as the architectural structure impacts the customer experience and the liabilities across the ecosystem. It is obvious that there are significant and closely woven design choices across the Labels and Governance Clusters, which would have a significant impact on the infrastructure, data and consent Clusters, in so doing enabling the delivery of value for consumers and removal of potential harms.

There is a dearth of Labels in the market, although there are some strong exemplars to build upon. However there are a number of Governance Structures which are evolving around common themes and ethical frameworks. These provide the individual with control, transparency and privacy and a fair value exchange. At the same time the Governance compliance regimes are by and large seeking to hold all of the actors accountable. Using one or some of these would provide a strong foundation for iterative testing across value opportunities, to test the ability to create sustainable value for consumers.

Standards have the ability to both follow and lead market growth, many of those needed are already in market in other sectors and in theory could be leveraged to enable the Health and Wellbeing value. There is a broad choice of technology solutions, some of which are interwoven with varying numbers of components from across the Clusters, e.g. Services such as Dataswift that provide Consent Management, Data Management which are embedded within a robust Governance Framework.

Summary of recommended Design Considerations

Below briefly summarises the recommendations made for the components that could form the end-state solution for a mature trust solution.

Components Clusters	Recommendations
Labels	• Consent labels indicating: 1. What data will be shared; 2. With whom will it be shared 3. For what purpose will it be shared 4. For how long will it be shared. • In addition, colour should be used to indicate contextual information such as risk levels. • Introduce a Kitemark to indicate to consumers which services are part of the trusted ecosystem
Consent	Consent structures that enable: • Consumer dashboard to view and revoke consents • Consents request via pop-up in health/wellbeing service flow • Consent receipts • Layer consents so that the services minimize data accessed to that needed for that part of the user journey, and promote "Fair Value Exchanges" • Avoid "dark patterns" to acquire consent
Data	• Data intermediary for both consent flows and data flows • Robust key recovery process • Encryption for data inflight and at rest
Above the Line Component Clusters	
Below the Line Component Clusters	
Infrastructure	• Analytics to be capable of running locally in consumers data store • Privacy Enhancing technologies to sit upon consumer data store • Data attribution capability
Standards	• Existing Standards: HL7 FHIR, ISO 27001, Privacy by Design • Standards gaps: A more standardised method is needed of mapping wellbeing data into FHIR. A method of mapping new insights onto clinical scales is needed.
Governance	• The following principles to be embodied in a rule-based code: 1. The individual's Control 2. The individual's Transparency 3. The individual's Privacy 4. The Fairness of the exchange 5. All actors Accountability • Consumer representative to sit on the governance body, alongside other stakeholders. • Consumer representatives to have the right to public disclosure • Governance body to license use of Kitemark and consent/privacy labels • Governance body to oversee compliance audits of members

7.1 Above the Line Components: Labels

Labels are the means to communicate with consumers, to enable them to make informed choices about whether to share their data. They appear in two forms:

- **Trust Seals** to inform if a service is part of the trusted ecosystem and abiding by its rules.
- **Consent labels** to inform what data will be shared with whom, for what purpose and for how long.

These labels need to be standardised to reduce the learning required by consumers to comprehend the information they are communicating.

7.1.1 Trust Seals

Most trust frameworks that are designed to build consumer trust have a Trust Seal e.g. British Standards Institute, Soil Association, the Marine Stewardship Council. These Trust Seals are copyrighted and can only be displayed by an organisation with the permission of the trust frameworks governing body.

Trust Seals perform a critical function for consumers by helping them identify quickly whether a given organisation complies with the undertakings required of them by that trust framework. In turn, this places pressure upon organisations to become members of the trust framework in order to build customer trust in their brand and help maintain and grow their market share.

In the sphere of data sharing, such thoughts are not new. In 2018 the Think Tank Reform1 recommended that the UK Government create a kitemark for data quality that is a,

> *"seal of approval… which indicates that data quality is satisfactory and that biases within data sets have been accounted for"*

More generally Trust Seals are available from the BSI, TRUSTe, Trust Guard, and Trust Lock which testify to an app or websites security and data handling practices. The NHS vets Health Apps for admittance to the NHS App Store and their criteria encompass data security and privacy. However, most Health and Wellbeing apps are not accessed via the NHS Store, which is limited to the UK.

No Trust Seals that we are aware of specifically relate to the sharing of data between organisations. We recommend that a Health and Wellbeing data sharing ecosystem establish a kitemark for display by its members.

7.1.2 Consent Labels

Consent labels are needed to help the consumer understand consent requests. They must include:

- What data will be shared
- With whom will it be shared
- For what purpose will it be shared
- For how long will it be shared

Ideally, these labels will be graphic/iconic in form and communicate additional contextual information such as risk level, e.g. how sensitive that data is or what level of security the requesting company operates.

Inspiration can be drawn from supermarkets food nutrition labelling.

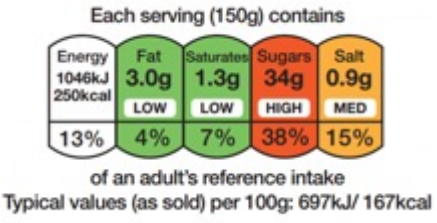


Figure 26:a An example of labelling

This combines factual information stated in the numbers with contextual information indicated by the colours. This approach has been extended by "The Hub of All Things" (HAT) for use by its data facilitators. Further work has been undertaken by the Kantara "Consent receipt" project (see figure 26b) and implemented by Data Facilitators such as Digi.me.

Here we can see the necessary information summarised and links from the icons to fuller descriptions if the consumer wants more information. Such Labels will be an important part of a trusted Health and Wellbeing data sharing ecosystem.

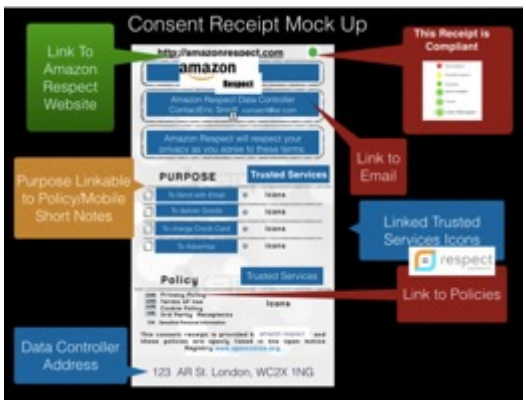


Figure 26b: A prototype consent receipt label

More recently a form of data labelling has been introduced by Apple with the release of iOS 14. Apple's labels articulate how Apps collect and use the consumer's data, these are shown in figures 26b, 26c and 26d.

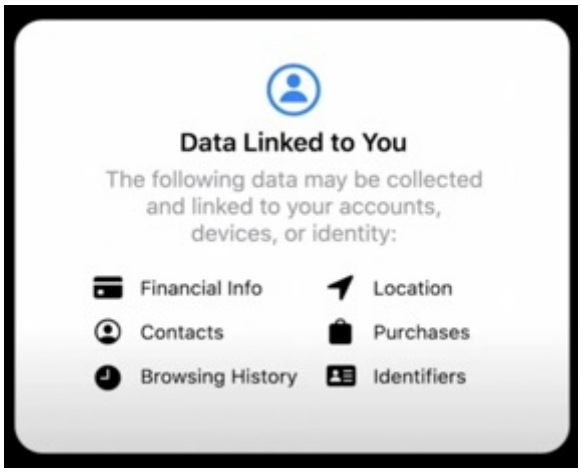


Figure 26b: An Apple label explaining the data an App accesses about the user

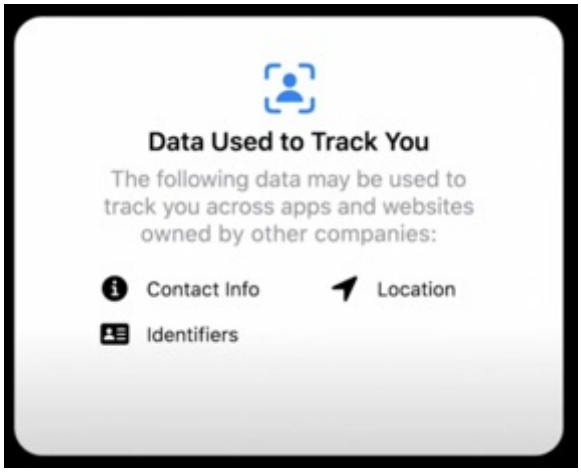


Figure 26c: An Apple label explaining the data an App uses to track the user

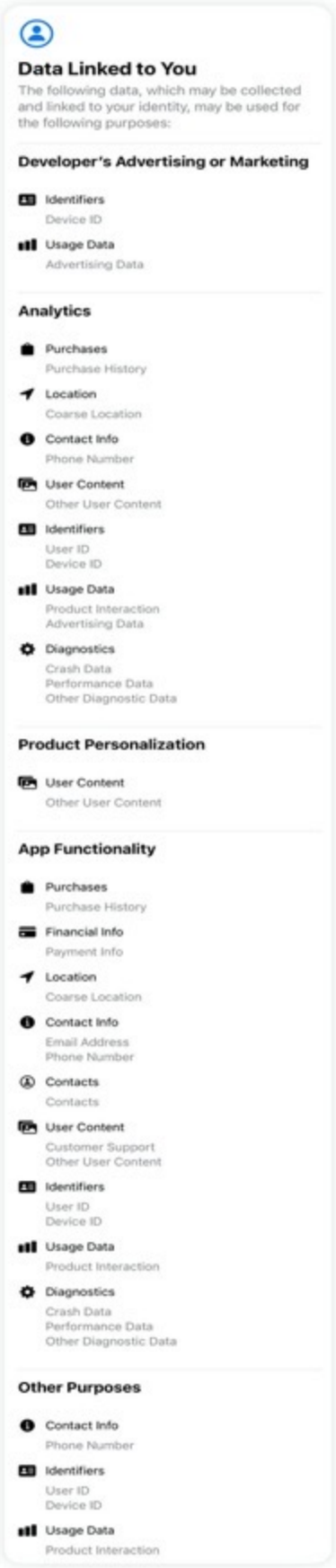
Apple divides their labels into three categories:

1. Data used to track you
2. Data linked to you
3. Data not linked to you

The introduction of Apple's labels has been generally well received and reflects a wider strategy by Apple to differentiate themselves from the other tech Giants, positioning their brand as primarily "on-the-side" of the consumer and against "sneaky stuff".

The introduction of the Labels has highlighted some striking differences between services. Given the functionality of WhatsApp and Signal are similar, the data labels make the differences in their data usage obvious to even the most casual observer.

WhatsApp's label



Signal's label

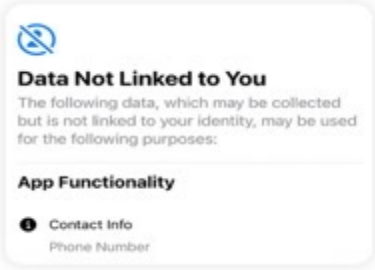


Figure 26d: An Apple label explaining the data used by the "Signal" and "WhatsApp" Apps.

7.1.3 User Experience Patterns

Finally, in our consideration of data labels, we will highlight the issue of “Dark Patterns”. These relate to where in the consumer journey and the context consent requests are made. Today a number of techniques are used to nudge consumers toward giving consent. These include:

- Privacy intrusive default settings
- More clicks required for privacy-friendly options
- Design colours and symbols
- Language leading to intrusive options
- Decisions required before a service can be used

Together these techniques are referred to as dark patterns and manipulate consumers into giving consent. Such UX patterns should be governed within a trusted data sharing ecosystem.

7.2 Above the Line Components: Consent

When considering flows of consent and data, we first need to decide what high-level architecture they will be embedded in. For data sharing architectures there’s a spectrum of options, with at one end direct sharing between the data source and service provider (e.g. Open Banking model), and at the other end architectures where data sharing is mediated by a Data Intermediary (e.g Digi.me, DataSwift, Meeco, Inrupt).

7.2.1 Open Banking Model

At first sight, the Open Banking model may seem simpler, as it has one less actor, however on deeper inspection it can be seen that this comes at the price of pushing complexity and risk onto the consumer, for the following reasons - In the Open Banking model:

- Consumer has no single place to see and manage their consents.
- With multiple data sources and service providers, the number of consents the consumer must give grows out of control , vs intermediaries
- The data has to be sent to the data provider to analyse the data and so “Honey Pots” of data end up with multiple providers, and algorithms cannot be pushed to the consumer’s data.

For these reasons, we envisage Data Intermediaries as a key driver of fairness, value and growth and will discuss the consent and data flows in what follows in that context.

7.2.2 Data Intermediary Model

Consents can be acquired by the Service Provider via an API call to the Data Intermediary. Typically this can invoke a pop-up window within the Service Providers user journey.

This pop-up explains the data sharing request and enables the consumer to accept or decline the request. The scope of information the request contains, must at least satisfy GDPR and include:

- What data is to be shared
- For what purpose
- For how long
- Who will be the data controller

Copies of the consent are both stored by the Data Intermediary and also sent to the Data Provider. Technologies such as “Data Receipts” are used to attest the consent records authenticity.

As part of any audit process, each enterprise is able to demonstrate how each consent record maps to the consented data processing within that enterprise. Critically this is accompanied by a set of processes that prevent data consented to for one purpose then being processed for purpose another. Critical features of the consent component include:

- Consent management dashboard
- Consent receipts
- Standardised consent labelling

7.2.3 Fair value exchange

Finally we will consider, how consent acquisition is intertwined with the principle of a fair value exchange. Value for the consumer can come in many forms, peace of mind, monetary, a better service, or benefits from third parties. What type and level of value to offer for the data is a proposition decision for the service provider, while accepting or rejecting it is the prerogative of the consumer. However, for such an exchange to be considered fair, both parties need to be able to make free and informed decisions.

In this context a free and fair decision implies that if the consumer were to reject the request, they should not be denied any services. If this is not the case, its not a request, rather a form of blackmail.

An informed decision requires both parties to be aware of the risks and benefits of sharing the data. To codify this concept would be complex, but reasonably reflected in the principle of “no sneaky stuff”. Service providers should ask themselves the question, “would the average consumer expect them to do that with the data”.

While ethical considerations recommend the above, so do practical ones. Consumers are less likely to give consent when the value exchange is unclear. This can best be addressed by layering consent requests. Rather than asking for lots of consents at once, services may more effectively build trust by asking for consent only when needed. This makes possible a clearer articulation of value to the consumer: “This item of data is needed in order to give you that benefit.”

In this way service designers need to think of consent as an integral thread in the consumer journey, rather than a ”bolt-on” consideration at the end or barrier to be overcome. Services that appear not to facilitate free and fair value exchanges, particularly if coupled to dark patterns, should not be admitted to a trusted data sharing ecosystem.

7.3 Above the Line Components: Data

As discussed above on consent management, we suggest there are good reasons to prefer the use of Data Intermediaries over the “open banking model” where the Data Intermediary on behalf of the consumer permits both the consent and data to be exchanged directly between data provider and data receiver.

This consented data exchange by Data Intermediaries can orchestrate in one of two basic ways.

7.3.1 Data Intermediaries’ data store

The Data Intermediary has a personal data store for each consumer. This data store also has the ability to run algorithms locally. The consumer connects this data store to each of their data sources, which then flow their data into their data store ad infinitum. The data store is heavily encrypted and can only be viewed by the consumer. Upon the consumer granting consent to a service provider to access certain data, the Data Intermediary permits the Service provider API access to that data only. In this way both the consent and data passes through the Data Intermediary.

7.3.2 Data Intermediaries: data B2B

In this option only the consent layer passes through the Data Intermediary, while the data is then sent directly B2B from the data source to the Service Provider. While different Data Intermediaries employ either option one or two, there seems good reason to prefer data store. In data B2B the consumer has no personal data store or ability to be given and run 3rd party analytics algorithms privately. This may require them to send all their data to each Service Provider.

This is an unnecessary privacy risk. Further when the service providers service is looking for changes in a consumers “state”, these data flows to the service provider need to be ongoing, which is inefficient. This makes option 2 poor for implementing digital customer experiences and journeys.

The architecture recommended above does much to enable organisations to better manage their data especially mitigating security risks. Each personal data store (typically cloud based) is separately encrypted. In effect a potential hacker faces all the usual problems breaking into the encrypted “storage”, but should they succeed, they only access one persons data. This reduces the hackers pay off for the same effort to the point where its rarely worth the computer time.

The main features we think are needed in the Data Storage component are:

- Strong encryption
- Robust key recovery process
- Ability to run algorithms within the store
- The support of Privacy-Preserving Technologies
- Data attribution and chain of custody

7.4 Below the Line Components: Infrastructure

In the previous sections, we looked at consent and data management components. Both these functions sit “above the line” i.e. are visible to consumers. In this section, we will look at the solutions that sit “below the line” which enable and enrich those consent and data management components.

The most important of these below the line components relate to the analytics infrastructure. To create value with data requires analytics, critically the Data Intermediary model supports the flow of data enabling multiple locations and opportunities for analytics to create value. Today the analytics are performed by the service provider, within their service infrastructure. However, as eluded to above, there may be distinct advantages to a “hybrid” approach where some analytics run locally within the consumer’s Data Intermediary and other analytics run centrally within the service providers infrastructure.

Such a hybrid approach enables privacy to be maximised, by minimising the amount of data shared. There are different degrees of sophistication that can be employed for the Data Intermediary analytics.

At its simplest, the service provider might push a simple algorithm to the Data Intermediary to answer a question like “is this customer female, aged 30 to 40 and located in London?”. The Data Intermediary would then gain consent to the output “yes” or “no” being sent back to the service provider.

At a more sophisticated level, the algorithm might be a Machine Learning model to predict credit risk, drawing on many variables contained in the Data Intermediary. However, if the data is not centralised by the Data Intermediary, how are such models to be built in the first place?

There are two broad approaches to answering this question. The first focuses on emerging distributed analytics techniques, which enable models to be built from distributed sets of data, by exchanging modelling parameters between the individual Data Intermediaries.

The second approach focuses on creating a sample data lake representing the population-level data, solely for the purpose of model building. Such a data lake can either be built from synthetic data or be subject to very robust security protocols.

The utility of the Health and Wellbeing data sharing ecosystem can be enhanced by ensuring the above analytic capabilities are available to the service providers. As such they should be considered in the detailed design process.

The main features we think are needed in the Analytics layer are:

- The ability for service providers to push consented algorithms to the Data Intermediary.
- The provision of privacy-preserving model building capabilities.
- The support of privacy-preserving technologies.

7.5 Below the Line Components: Standards

To construct a trusted Health and Wellbeing data sharing ecosystem there are a number of areas of standardisation to consider. For an MVP these include:

- Data ontology
- Security
- Privacy by design
- AI ethics

API Standards must also be included for a successful ecosystem, these are standard technology solutions now available in market.

7.5.1 Data Ontology

Over the last decade, a great deal of work has gone into standardising Health Data ontologies as part of the journey toward Electronic Health Records. In the UK there are a number of institutions engaged in standardising health data (CQC, NHSD, NHSE, NHSI, NHSx, PRSB etc), but the intention is to converge on a common framework centred on the “Health Level 7” (HL7) framework which has spawned the “Fast Health Interoperability Resource” (FHIR) standard. This combines a data ontology with an API standard to transfer the data.

While there is a fair degree of standardisation in the ontology and API’s for clinical healthcare data, the picture is more uneven for consumer Health and Wellbeing data. Some service providers such as the Apple Watch have implemented FHIR, while most others such as Fitbit, Garmin etc record data in a propriety data model. The net result is to make the integration of consumer Health and Wellbeing data with electronic patient records problematic. This in turn limits the analytics which can be run against the combined data. This represents a huge loss of potential value. How can one determine if a signal in the consumer data is indicative of later outcomes recorded in the clinical data?

To overcome these issues a number of proposals have been developed to map the data from both consumer and clinical sources into a common data model. While a number of challenges remain, a combination of APIs and Semantic Web technologies appear a potential solution. To maximise the value of a Health and Wellbeing ecosystem, interoperability with the clinical health data ecosystems is desirable. Consequently, identifying and promoting an interworking solution should be part of a Governance Body’s remit.

When the data has been mapped to a standardised model, the second level of standardisation issue emerges. Based on the data produced by a device, a service provider might draw an inference e.g. “your depressed”, but how is this to be interpreted by a clinician? Clinicians use well defined clinical scales to qualify and quantify a condition. These scales are driven by clinical data which differs in scope from consumer Health and Wellbeing data. Take for example a wearables service provider who has conducted a “big data experiment” showing a correlation between a change in activity and depression.

When the consumer presents at their doctors saying they have been told they're depressed, what is the clinician to make of it, other than to start from scratch and collect clinical data that they can actually interpret? At present, there are few certification bodies to endorse the inferences drawn from consumer devices and none actively trying to align those inferences with the clinical scales needed by clinicians. This is another missing component that could add significant value to a Health and Wellbeing data sharing ecosystem. There are a number of existing bodies that might usefully extend their remit to close this gap. In the UK these include NICE and NHS-x. Such a change in the remit for those bodies is beyond the scope of a data-sharing ecosystem, and so best viewed as a policy recommendation.

7.5.2 Security Standards

Turning to data security standards, we note a range of well-established standards already exist. For Healthcare data the NHS Digital "Data Security Standards" represent a robust set of practices that will evolve as new threats develop. Internationally ISO 27001 and in the US HIPPA both define relevant data security standards.

7.5.3 Privacy by Design

In addition to security standards, risks associated with Health and Wellbeing services can be mitigated by developing the services using Privacy by Design principles. These principles are:

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality — Positive-Sum, not Zero-Sum
- End-to-End Security — Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy

These principles build privacy thinking into the service design and organisational structure. They ensure data is not unnecessarily collected, and removed when no longer needed. They encourage service designers to think about incorporating anonymisation and privacy-preserving technologies into their service design. One of the implications for our considerations here is to invite us to think about different architectures that enable distributed vs centralised data and the possibility of sending analytics algorithms to the data rather than centralising data for analytics.

7.5.4 AI Ethics Standards

Finally, we will touch on the emerging field of AI Ethics standards.

This is an active area of work at the moment globally. A number of AI ethics frameworks have been developed, usually focusing on the following principles:

- Transparency
- Justice and fairness
- Non-maleficence
- Responsibility
- Privacy

Work in the UK is led by the CDEI, Alan Turing Institute and HMG's Office for AI. If service providers within the Health and Wellbeing data sharing ecosystem undertook AI practices that were not aligned with these principles, it would in all likelihood undermine consumer trust. As a consequence AI ethics should be incorporated in the ethics code and an AI ethics standard adopted by the governance body. In doing so, it's critical to ensure the ecosystems ethics are kept simple enough to be effectively communicated to end consumers.

7.6 Below the Line Components: Governing Frameworks

Governance plays a critical role in the creation of a data-sharing ecosystem that consumers trust. In many ways, the question of what's the right approach to governance is really two components folded into one, Ethics and Frameworks.

The first question is "to what ends is the governance in place", that is what ethical position is it trying to instantiate. The second question is then one of means, rather than ends, that is how does the governance instantiate that ethical position?

We will start by exploring the ethics that the governance needs to embody, in particular the differences between "rule-based" and "principle-based" approaches.

7.6.1 Ethics Principles

Human Rights are widely accepted ethical norms, distilled from earlier political philosophy during the 1950's, into the form and legislative structures that we know today. Personal data plays a role in considerations of privacy and equality. In the 21st Century, the EU has played the leading role in defining and enacting legislation to give the individual agency over their personal data. This an extension of earlier conceptions of human rights, aimed at defending those core values, in today's digital societies.

The locus of the EU extension of personal data rights, through GDPR, EU Data Strategy and the EU proposed Data Governance Act, has been to give the data subject control over what is done with their data. While the concept of ownership is a slippery one when applied to data, the zeitgeist of this trajectory is increasingly clear in consumers minds: "people control their data". While this is not yet fully embodied in law, it would seem to be fighting against the tides of history to adopt a different ethical starting point.

A number of ethics frameworks have been developed over recent years enshrining consumer control over their data to facilitate the sharing of personal data. These include:

1. HAT / DataSwift Ethics Code
2. MyData Global
3. WEF Personal Data Sharing Code of Conduct
4. ODI data ethics canvas
5. Code of Conduct of NHSX
6. EU Data Governance Act

Dataswift (nee HAT)

Dataswift is a Data Intermediary which grew out of research by 6 UK universities from 2013. HAT is in many ways the original thought leader in the creation of an ecosystem with a tight coupling between their ethical principles, governance, liability model, technology and consumer privacy communication. Their ethical code is built around the following principles:

UX Design: Ethical data means ethical by design, rather than navigating complex legislation and the ever-increasing challenge of trust within customer relationships once you've collected it.

Legal Ownership: Ethical data means complete legal ownership of the data by the individual and equitable first-party contracts for sharing and usage.

Data Sourcing: Ethical data means data that is responsibly sourced by organizations directly from their customers through tech infrastructure the individual owns themselves.

Processing: Ethical data means edge processing and computation enabled by the individuals themselves via a personal data server.

In short, HAT sees ethical sharing as rooted in a system design and operation that engages the consumer, gives them control and offers a fair exchange of value.

MyData Global

A not-for-profit organisation founded to support the emergence of an ecosystem for personal data sharing which adheres to a particular set of ethical and design principles. These principles are articulates in their "MyData Declaration", whose key principles share much in common with Dataswift's, but with some important differences. Mydata defines the ethical principles for an ecosystem in which Data Intermediaries are used by consumers to manage and control the sharing of their data. Their key principles include:

1. Human-centric control of personal data
2. Individual as the point of data integration
3. Individual empowerment
4. Data portability, access and reuse
5. Transparency and accountability
6. Interoperability

These are similar to Dataswift principles, although MyData mandates these principles be instantiated through a different technical architecture for the data intermediaries. Whereas HAT fuses the consumer's consent tool to a private space in which the consumer can aggregate, store and process their own data, MyData mandate a separation between the consent and data use layers, to prevent perceived conflicts of interest.

For the application of advanced models utilising broad Health and Wellbeing data, it appears undesirable to require the consumer's data to be aggregated by each service provider, in order to run their service.

WEF Personal Data Sharing Code of Conduct

This code is currently under development and is due to be made public in Autumn 2021. Private communication suggests it will be aligned to and build upon the principles of GDPR. Further, it will make all players within the supply chain responsible. The juxtaposition of these two drivers, in practice, is likely to require the use of Data Intermediaries.

The ODI Data Ethics Canvas

This is a tool produced by the Open Data Institute to help service providers design services to use data ethically (see figure 28 below). It's analogous to some of the questions that one might ask in a privacy impact assessment, but takes a broader perspective of the ethical issues, not least since it applies to all data, not just personal data. The canvas is shown in the figure below:

Figure 28: The ODI Data Ethics Canvas

The canvas is primarily intended to help service providers ask the right questions in a structured way rather than advocating specific outcomes.

NHS Code of Conduct

The NHS has built upon the ethical principles for data initiatives, developed by the Nuffield Council on Bioethics, to create their Data Ethics Framework for data-driven health technologies. The Nuffield Council has identified 4 principles:

- The principle of respect for persons
- The principle of respect for established human rights
- The principle of participation of those with morally relevant interests
- The principle of accounting for decisions

The NHS Data Ethics framework offers a series of questions and tests that can be applied to a given service to explore and judge the services adherence to these fundamental principles. In particular, it is focused on:

- Transparency
- Accountability
- Fairness

This approach, like that of the ODI Data Ethics Canvas, is intended to be applicable to a wide range of services and circumstances. Consequently, it avoids mandating specific actions, since the viability and morality of any action is context-dependent. Rather, within the framework, it helps identify ethical issues and ensure proportionate measures are taken to mitigate those risks.

EU Data Governance Act (as proposed 2020)

This act is currently passing through the EU Parliament. Amongst other things, it establishes a legal basis for Data Intermediaries. One of the ethical points it addresses is the potential for a conflict of interest if a Data Intermediary both offered:

- Data Intermediary services
- Revenue generating services that used the individual's data, beyond those needed to perform the tasks of a Data intermediary.

The Act foresees a risk that such an intermediary would have a conflict of interest, torn between acting in the consumer's best interest and promoting their other revenue-generating service. Consequently, the Act mandates a structural separation between entities acting as Data Intermediaries and those offering services utilising the consumer's data.

Summary

Broadly we see a common set of ethical principles underlying the different personal data sharing frameworks. These include maximising:

- The individual's Control
- The individual's Transparency
- The individual's Privacy
- The Fairness of the exchange
- All actors Accountability

Beyond these principles, we can group the framework's approach to delivering on the ethical principles into two groups: 1) Rule-based; 2) Principle-based. Into the first group fall Dataswift and MyData, and into the second falls the ODI Canvas and the NHS Framework.

In part, this divergence reflects a need to be less specific and rule-based when the scope of the framework's applicability is very broad e.g. all digital health-based services. When the scope of the framework is narrower e.g. consent-based data sharing, we see the frameworks being more specific and rule-based.

Given our task at hand is primarily to develop a high-level solution to address consumer mistrust in sharing their Health and Wellbeing data, we note:

- Our task is narrow and specific. It's about the efficacy of sharing the data, not the efficacy of broader service.
- Specific guarantees are more likely to engender trust than less specific ones Consequently, we recommend a rule-based approach to an ethical framework.

7.6.2 Governing Frameworks

Ethical principles alone are unlikely to engender consumer trust, without evidence that they are being interpreted and implemented in the consumers best interests. These are both critical functions of the Governance process, which must ultimately act as

the “trust anchor” in the eyes of those who rely on the data sharing process. At its heart, the governance process must achieve three things.

- Firstly, to translate the ethics principles into a code that is more granular and implementable by service providers.
- Secondly, to establish some system to ensure that those service providers who sign-up to the code adhere to it.
- Thirdly, to establish some way of communicating the above to consumers and service providers.

In short, the governance framework must decide on: representation; compliance and; communication to the market.

Representation in Governance

Consumers are well aware of the ability of highly paid corporates lawyers to find ways to adhere to the letter of the law while breaking its spirit. No matter how worthy the ethics principles, why should a consumer trust that there’s “no sneaky stuff” going on?

One approach is to give consumer representatives a role in the governance process. Such representatives need to solely be concerned with the consumers best interests and have no conflict of interests. Further, they need some way to publicly warn consumers if they feel the governance process is no longer protecting consumers. A number of examples of such governance structures exist today, from which several flavours can be decerned. Examples include:

- aNewGovernance
- HAT Community Foundation
- MyData Global
- Marine Stewardship Council
- Soil Association, organic food certification
- NIHR “Going the extra mile”

We will briefly compare and contrast each of the above, before drawing out the main “flavours” of these different approaches.

aNewGovernance

An emerging international association bringing together public bodies, associations, academics, start-ups, and corporates from all over the world.

The goal is to create a governance body as a Public-Private Partnership (PPP) for Personal Data Sharing.

This initiative accompanies the shift to a fair data economy, especially in the context of the GDPR and of the European Data Strategy with the development of Data Spaces (health, skills, mobility, finance, agriculture, energy, administration, green deal).

The association's aim is to help build those Sectoral Data Spaces in their Governance and Personal Data dimensions, as well as the Personal Cross-Sectoral Data Space.

Although kickstarted in Europe, it puts a great emphasis on the international dimension. The objective is to encourage human-centric fair use of data moving away from both All-State and Platform-centric (Winner takes all) models.

The vision is a global human-centric personal data network in which all organisations take part and where data can easily flow from one organisation to the other under the person's complete control and transparency.

HAT Community Foundation (HCF)

This oversees Data Facilitators who use the HAT technology, such as DataSwift. The HCF is a separate legal entity that interprets a consumer-centric ethics code and establishes rules by which its Data Facilitators must operate. Compliance with the rules by the parties using the Data Facilitators (data sources and relying services) is audited by the Data Intermediaries, but HCF, in turn, audits the Data Intermediaries performance of this task and may act as an arbitrator in case of disputes. The HCF board has representation from the Data Intermediaries but is dominated by consumer representatives. At present these are mainly academics, but reform to increase diversity is underway.

MyData Global

MyData Global is a non-profit that has developed a consumer-centric ”pledge” that participating organisations are invited to adopt. To date, over 100 organisations have become members. Data Intermediaries can apply to be certified as a “MyData” Operator.

To be approved they must demonstrate that they abide by the pledge by meeting a number of criteria. About 30 Data Facilitators have been certified and so may display a certification logo. In addition, individuals can sign up as members and over 400 people have done so.

The steering group has two representatives of organisational members and two representatives of individual members. Beneath this sits the Board which is dominated by academics and industry luminaries.

Drawing on experience we find a number of examples in markets where trust in the ‘system’ is needed.

Marine Stewardship Council

This is a non-profit organisation whose aim is to promote sustainable fishing. They develop fishing standards and operate a kitemark that may be used on food products produced by sustainable fishing in accordance with their standards. Their governing body is the Board of Trustees. Membership of this board is designed to represent different stakeholder groups: Fisheries, Food producers, Conservationists and Academics. In addition, it tries to ensure members are from diverse geographies. New members are nominated by existing members.

Soil Association, organic food certification

The Soil Association is a charity established in 1946, aiming to advance the education of the public by promoting a full understanding of the vital relationship between the health of the plants, animals, people and the environment. As part of this work, they have established standards and a certification process for the production of organic foods. Food producers and farmers can undergo certification to enable them to display the Soil Association Organic Food kitemark on their product. The certification standards and process is operated by a separate legal entity that is wholly owned by the Soil Association. Their standards are aligned to, but generally exceed other EU and Global organic food standards. The ”Trust Anchor” for this certification process is rooted in the reputation of the Soil Association, rather than any board whose membership is representative of various stakeholders.

NIHR “Going the extra mile”

This is not a governance structure in the sense of the ones considered above, but rather a set of recommendations by The UK’s National Institute of Health Research for the participation of patients and citizens in the governance of clinical trials.

Through evidenced-based research the NIHR suggest public engagement in trial governance bring two key benefits: 1) the transparency builds trust and makes trialists easier to acquire; 2) the public bring a different and useful perspective on the academic research.

They go on to consider the best way to involve public representatives in the governance process bridging the gap between “deep science” and making it comprehendible to the layman.

Reflecting on the above we see three basic approaches to founding consumer trust in a Governance Frameworks:

1. Representation of industry stakeholders (e.g. Marine Stewardship Council)
2. Representation of industry stakeholders and consumers (e.g. HAT, MyData and NIHR)
3. Trusted advocacy group (e.g. Soil Association)

Given the perception and reality of corporate misbehaviour with personal data, the first of these approaches is unlikely to be convincing for consumers for personal data sharing. The third works best where there is clear longstanding ethical leadership in a field, which is not the case for personal data. The second is most likely to be successful where the Governance Framework has representatives of each stakeholder group, including consumers as active participants.

7.6.3 Governing Compliance

How can the public trust that the code developed by the governing entity is actually being implemented? This reduces to three questions:

1. Do you really need a compliance process?
2. How lightweight can the process be?
3. Who operates the process?

On the first of these, you could imagine each organisation deciding which information to publish to demonstrate their compliance. Or a free market of “auditors” growing to certify the organisation against their own interpretation of the code. Both of these outcomes burdens the consumers with work trying to weigh the evidence of compliance. This seems unlikely and so unsatisfactory. We conclude you do need a compliance process.

So how heavy or lightweight does the compliance process need to be? We can envisage a spectrum where at one end an organisation self certifies and further checks are only undertaken when consumer complaints arise. In the middle lays initial certification by independent bodies. At the far end lays initial certification by a body that also conducts ongoing compliance checks. Where on this spectrum should a system governing the sharing of Health and Wellbeing data fall?

Would we ask a consumer to trust an organisation of which we have had no independent oversight? Such an approach appears unlikely to engender consumer trust and so some initial compliance audit seems needed. The degree to which follow-up checks are needed and how consumer complaints might trigger these follow up checks is a second-order problem that can be addressed in a later design phase.

This takes us to the third of the questions: Who operates the process?

Clearly, the Governance body owns the process, but they then have the option to either operate the process themselves (e.g. the soil association and MyData) or to certify and appoint auditors to undertake the process on their behalf.

There are pros and cons to both approaches, with perhaps the scale of the expected number of participants being the deciding factor. If a large number of geographically disperse organisations need certifying, then 3rd party auditors is likely to be the only way to scale the process rapidly. If a slower expansion is envisaged, then there may be merit to the governance body operating the process in-house to refine the process and then considering external certified auditors at a later date.

7.6.4 Market Communication of Governance

Ultimately the governance process is striving to give the consumer a reason to trust the data sharing process, while achieving this in a way that supports the needs of the other commercial stakeholders. This requires it to both develop a data-sharing system that is agreeable to consumers and also clearly articulate two things:

- What those “rules of the road are”
- When those rules are in force

The first of these is rooted in an articulation of the ethical principles. These need to be expressed in a way that’s short and clear. Standardised text delivered to the consumer through participating brands is one useful thread in a strategy to raise consumer awareness of the “trusted data sharing ecosystem”.

The governance body will also need to be responsible for a broader go-to-market media strategy.

The second issue relates to communicating to consumers which brands are part of the ecosystem and when the rule of the ecosystems apply. This is essentially the function of a kitemark, which certified organisations can display as part of their customer communications. Part of the governance function purpose should be to manage and defend the integrity of such a kitemark.

8. The Way Forward

8. The Way Forward.

There is a unique opportunity for innovators to collaborate in accelerating the trusted health and wellbeing data ecosystem of tomorrow.

The pace of change and market size of the opportunity for the use of Consumer Generated Data to support and enable the Health and Wellbeing of individuals are undeniable. The systemic barriers similarly are apparent.

Resolving these barriers calls for an agile development of a Trusted Personal Data Sharing Solution which leverages existing market components. Rapidly and iteratively maturing to support a vibrant, open and valuable data sharing ecosystem.

8.1 MVS design considerations

The scope, development principles, and objectives of phase 2 are designed to support fast paced progress.

8.1.2 Scope

To enable focus on where demonstrable value can be rapidly created the scope of the design of the MVS has been bounded.

	In Scope	Out of Scope
Value Focus	Prevention Adherence management Value of the data sharing	Critical Health Treatment services Value of the services
Data	From across the lives of individuals including consumer generated Health and Welling data	Regulated Health data
Use	Outside the clinical setting NB helps define the scope of the clinical setting of such data	Needs of vulnerable or disadvantaged consumers
Consumers	Fit and Well Unfit Focused on wellbeing regime adherence	Sick Requiring critical health treatment

Figure 29: Minimal Viable Solution Scope

The following set of design principles aim to align to market opportunities, avoid early complexity and enable stakeholders to purposefully engage and invest in the development of an MVS.

8.1.2 MVS Design Principles:

- Empowering individuals with their data to enable personal wellbeing.
- Enable prevention of illness and adherence to treatment management as the primary use cases.
- Relevant to consumers who are Fit and Well, Unfit, or focused on wellbeing regime adherence.
- Data is enabled from multiple sources across an individuals life.
- Inputs into data's scope of use within the clinical setting.

The following table provides an initial scope which will be developed in collaboration with the MVS participating stakeholders.

8.1.3 Development Principles

The following provides principles for the development and design of the MVS

- Uses market challenges to test a set of proof points which are designed to unlock the value in the flow of trusted data.
- Using qualitative testing with consumers, businesses and ecosystem stakeholders.
- Undertaking quantitative analysis and testing to support investment decisions.
- Doesn't reinvent the wheel, uses what's available in market and where appropriate modify existing.

8.1.4 Objectives and Proof Points

The Minimal Viable Solution feasibility objectives and proof points will form the foundation.

1. Objective: Consumers can trust the data ecosystem and ultimately share more data

Proof Points:

a) We understand the drivers for trusted data sharing.

b) The solution is architected to nurture trust in the context of collecting the data and using the data.

c) We understand which MVS components contribute most to nurturing trust.

d) We understand trust sensitivities around sharing non H&W data within a H&W setting.

e) We understand the propensity to share data in different contexts e.g. wellbeing prevention vs wellbeing adherence.

2. Objective: To test the maturity of the market components

Proof Points:

a) Assessed the level of maturity and market readiness of the components.

b) Enables personal algorithms to be run locally.

3. Objective: Mature market components can be combined to create an MVS

Proof Points:

a) Mature market components can be technically combined.

b) The MVS creates a secure solution.

c) The MVS creates a usable solution for consumers.

4. Objective: Scope the market appetite for a Minimal Viable Solution

Proof Points:

a) Removed constraints on designing trusted User Experiences.

b) Provides protection for businesses brand reputation in personal data use.

c) There is a need for an MVS to support product roadmaps.

5. Objective: MVS drives additional value creation

Proof Points:

a) Consumers get better value from their data.

b) User Journeys in sandbox participants business will be more effective for consumers and businesses, contacted at the right time, right place, right offer.

8.1.5 Stakeholders

The development of the MVS requires a number of market stakeholders from across the ecosystem to make strategic investment decisions, provide guidance and insight, and to action market making activities.

The table below (figure 30) summarises the stakeholders and the important components they bring and role they play in the development of the MVS.

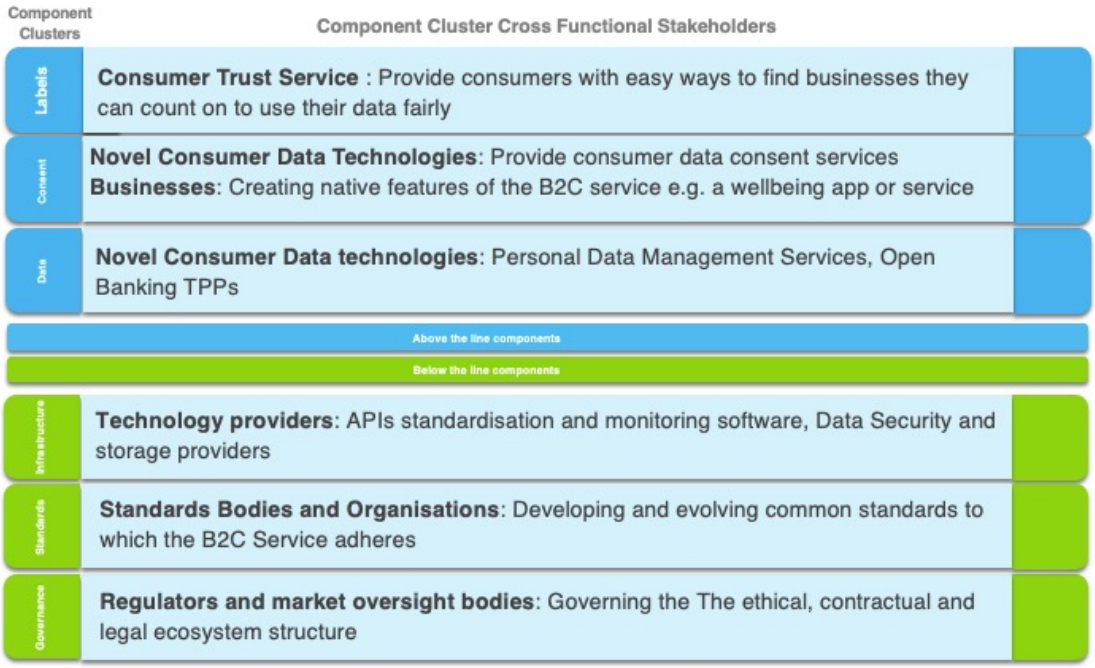


Figure 30: Minimal Viable Solution Stakeholders

8.2 Innovation Approach

Innovation of the MVS for a Trusted Personal Data Sharing Solution requires a broad programme encompassing a number of market requirements. This will bring together the multi-functional stakeholders to learn together and run rapid test and learn iterations.

8.2.1 The Sandbox

The Ctrl-Shift Sandbox uses MVS Challenges, bringing together an End User Panel and Advisory Group to design the requirements, with a Sandbox team to configure the components upon which tests are run. The tests rapidly inform the design of the MVSs' Operating Model, Playbook and Infrastructure Roadmap.

Rapidly iterating and testing with end users and the business community, each iteration of the MVS

8.2.3 Outcomes

The outcomes will be a design and prototype for a Trusted Personal Data Sharing Solution for Health and Wellbeing. It will be tested with users covering the Trust Labels solution, Governance structures and Standards, Data Access and Consent best of breed components integration. It will inform the understanding of the applicability in different contexts. A cohort of relevant companies with the opportunity to operationalise the solution will take part.

8.2.4 Business Participants

Participating businesses will benefit from working alongside an ecosystem of stakeholders with a breadth of multiple challenges and access to a breadth of ecosystem expertise, and best of breed.

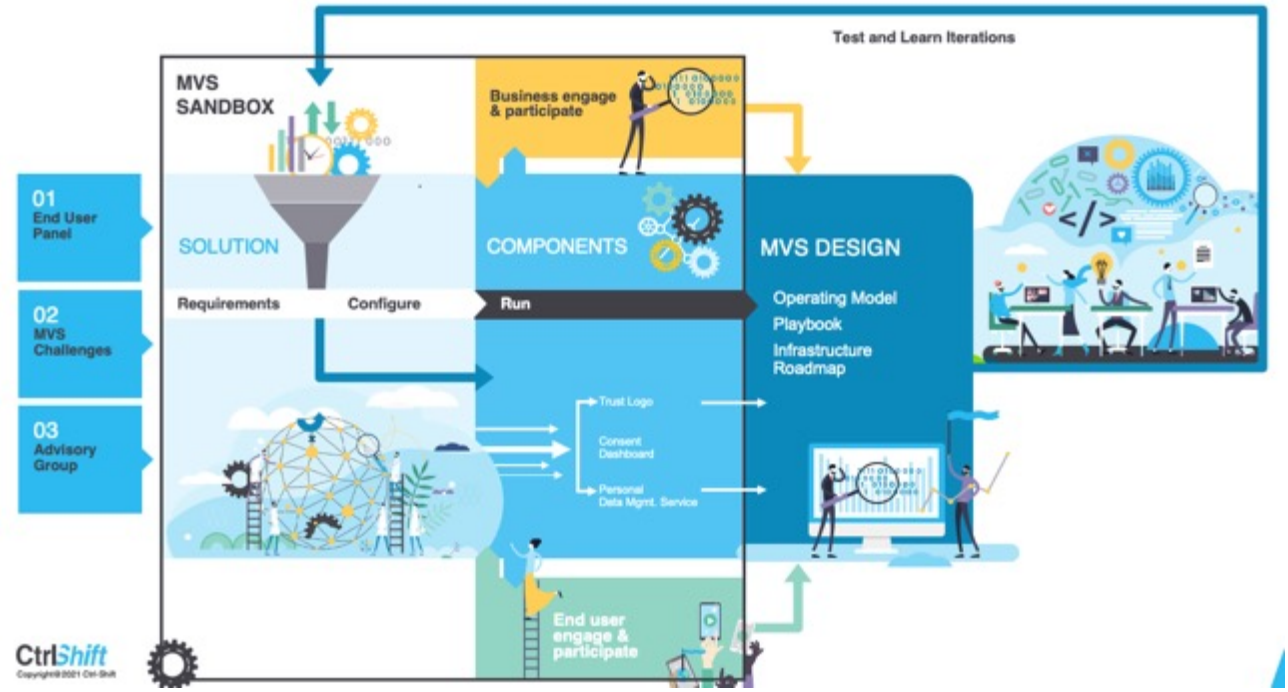


Figure 31: Sandbox iterative design model

Challenge iteration of the MVS informs the next, building over time an increasingly robust MVS Design, answering the requirements of multiple Challenges and enabling the configuration and design of the MVS to incorporate the needs of multiple participants and the varying requirements of the challenges.

8.2.2 MVS Challenges

The MVS Challenges may be a combination of functional requirements such as User Journey Orchestration or the Design of Federated Learning Solutions, or specific value opportunities. Participating businesses will bring the MVS Challenges from a cross-section of the ecosystem and selected based on the Design Principles, Objectives and Proof Points.

components in the Sandbox. Full reporting on the operations of the Sandbox and the MVS Design iterations will be designed to support business solutions.

8.3 Funding

Funding for Phase 2 of the Sandbox is a collaboration between stakeholders, each providing a combination of funding and capabilities to support the development of a Minimal Viable Trusted Personal Data Sharing Solution.

Future funding will be sought to support the ongoing development of the Trusted Data Sharing Solution and ecosystem.

Glossary of terms

Term	Description
Component	A capability that may contribute toward the overall trust solution
Component Cluster	Components Clustered together to offer broader functionality which may contribute to the overall trust solution
Consent	The consumers legal agreement for the data to be shared, acquired in the manor specified in GDPR or locally applicable legislation
Consent Dashboard	A web or app page that lets consumers view the consents they have granted to one or more services and offers them the ability to grant or revoke consents.
Data Access	The ability for the consumer to access and view their own data. This is most typically achieved by enabling them to aggregate their data in their private data space on their device or private cloud.
Data Analytics	The ability to analyse data, either at the individual or population level to gain factual or statistical insights
Data Provenance / attribution	The capability to determine the origin and authenticity of the data by the party who receives and relies upon the data.
Data Facilitator	This is a third-party intermediary who acts on behalf of the consumer to help them manage the sharing of their consents and/or data
Data Labels	These are labels within the consent request that articulates the terms of the requested data sharing in a standardised way e.g., through icons.
Data Trust	This is a legal entity with whom consumers share their data for a defined purpose. The Data trust typically anonymizes their data and draws insights from the aggregated population level data.
Federated learning	This is an analytic approach that enables the building of population level models based on distributed data repositories, without aggregating the data
Homomorphic encryption	This is a type of encryption upon which analytics can be preformed on the data in its encrypted state, which returns the same results as if the unencrypted data were used.
Kite Mark	In this report we use the term to refer to the totality of the trust solution, including the Trust Seal and all other components
Model building sandpit	This is a data storage in which data is aggregated in order for machine learning models to be built.
Open Banking Model	This refers to the Open Banking Implementation Entities architecture, in which the consumers consent for data sharing is given directly to the business which holds the data, without the use of a data intermediary.
Privacy Enhancing Technologies	These are a class of technologies which manipulate personal data to make it more difficult to identify an individual from their data.
Privacy by design	This is a set of principles and practice that embeds privacy into the design of a service
Trust Seal	This is a logo backed by some code and governance that indicates certification to some standards by those services displaying the Trust Seal.


CtrlShift