Sharing is caring?

Could data-sharing improve the support provided to customers in vulnerable situations?

RESEARCH REPORT

April 2018

University of BRISTOL
Personal Finance Research Centre

Table of Contents

Executive Summary 3
About this research 11

Part one: what's the context for this research?
Collecting data from individuals – current practice 15
The regulatory context 16

Part two: what's the case for greater data-sharing between organisations?
What's the case for greater data-sharing between organisations? 19
How common are disclosures of vulnerable situations? 20
How could data-sharing benefit consumers? 26
What are the risks to consumers of greater data-sharing? 30
What are the trade-offs for consumers? 32
How could data-sharing benefit organisations? 34
A summary of potential risks and benefits 36

Part three: a blueprint for data-sharing between organisations
A blueprint for data-sharing between organisations 39
Building block 1 – data disclosure 40
Building block 2 – data capture 43
Building block 3 – data hygiene 48
Building block 4 – data-sharing 50
Building block 5 – data control 55
Steps towards greater data-sharing between organisations 58

Appendix 59
Endnotes 60

This report was prepared by Professor Sharon Collard (Research Director), Jamie Evans (Research Associate) and Chris Fitch (Honorary Research Fellow), Personal Finance Research Centre, University of Bristol.

Acknowledgements We thank Barrow Cadbury Trust for grant funding this project; the Money and Mental Health Policy Institute for giving us survey access to its Research Community; the Research Community members who kindly completed the survey; and the industry and consumer experts who gave up their time to be interviewed.

University of BRISTOL
Personal Finance Research Centre

Barrow Cadbury Trust

Executive Summary

This report asks whether greater sharing of data between financial services firms can improve their ability to identify and support customers in vulnerable situations. It considers how such data-sharing could work in practice, and presents 'building blocks' for the industry to consider if it is to take forward increased data-sharing.

The report is based on new research which comprised of an **evidence review** of academic papers, research reports and policy documents from sectors including financial services, health, utilities, and government services; an **online survey** completed by 244 members of the Money and Mental Health Policy Institute's Research Panel, who all have first-hand experience of mental health problems; and 18 **expert interviews** with representatives from financial services, the energy and water sectors, the advice sector, and data specialists.

Why is this topic important?

Every day, firms in the financial services industry encounter a large number of customers in situations that may make them 'vulnerable'. These individuals, due to their personal characteristics or wider circumstances, can be particularly susceptible to detriment if the organisation fails to take their situation into account.

At present, organisations usually only become aware of such situations if the customer (or a third party acting on their behalf) tells them about it. This means that if a customer doesn't disclose the situation to any, or all, of the organisations they encounter they will not receive support they may be eligible for.

Data-sharing between organisations may offer a way to ensure the customer gets all the support they need, without requiring them to have the same conversation with multiple different organisations.

Disclosing personal information can be draining – whether it's about a health issue, a bereavement or some other difficult situation.

Rather than having multiple, similar conversations with different firms, what if the first firm that an individual speaks to could simply notify all the others?

Executive Summary

Is there a need for data-sharing?

When exploring the viability of any intervention, we should first ask ourselves: is there a need for it?

To answer this question for data-sharing, we begin by considering the frequency with which consumers already disclose information about vulnerable situations to financial firms, and the extent to which they are required to disclose to a number of different organisations.

Our research finds that it is not uncommon for consumers to disclose vulnerable situations to financial (and other) organisations (**see p.20-25**):

- 44 per cent of respondents in our survey have told their bank about their mental health condition; 38 per cent have told other lenders; and 63 per cent have told a money or debt adviser.
- Over a quarter of those surveyed had told more than one lender about their mental health problem (26 per cent), or more than one money or debt advice organisation (also 26 per cent).
- Our previous research found that debt collection staff receive a median of 15 disclosures of a serious physical illness from customers or their families each month, 12 disclosures of a mental health problem and nine disclosures from a bereaved customer or third party.

In other words, there may be a large number of consumers who are already disclosing sensitive information about vulnerable situations to financial services firms. These individuals and their families could be affected by any move towards greater data-sharing.

44 per cent of those with mental health problems that we surveyed had told at least one bank about their condition and 38 per cent had told at least one other type of lender.

Over a quarter (26 per cent) of all those surveyed with mental health problems had told more than one lender about their condition.

Executive Summary

What are the benefits and risks of data-sharing?

As the Table on page 6 shows, there are a range of possible benefits associated with increased data-sharing, but also a number of risks that would need to be mitigated against in the design of any data-sharing scheme (**see p.26-37**).

In terms of benefits to consumers, increased identification of vulnerability by firms could lead to more consumers receiving relevant help and support from organisations, or products more tailored to their needs. Data-sharing may also mean that fewer consumers would have to explain their situation to multiple firms, something that our research shows can be very challenging – as evidenced by the fact that 67 per cent of respondents to our online survey found it 'very' or 'quite difficult' to disclose their mental health problem to their bank, as did 65 per cent of those who disclosed to another creditor.

From our expert interviews, it was clear that financial services firms also recognise the benefits of data-sharing and are interested to explore opportunities and learn from other sectors. At the same time, they are understandably nervous about how sharing such sensitive data would work in practice and acknowledge the risks of such data being mismanaged or misused.

Ultimately, there are trade-offs associated with increased data-sharing (**see p.32**). The majority of our survey respondents (84 per cent) said that – providing certain conditions were met – they would be open to firms sharing information with other firms about their mental health condition.

Our survey showed that 67 per cent of consumers with mental health problems find it difficult to disclose their mental health problem to their bank.

"Having to explain to banks/ other people you don't know but you are forced to explain is very stressful and unnerving… I come away feeling guilty and angry with my past… it made me feel suicidal." **(Survey respondent)**

84 per cent of consumers with mental health problems would be open to firms sharing more data with one another – providing certain conditions are met.

Executive Summary

Table - Potential benefits and risks of data-sharing

	FOR INDIVIDUALS	FOR ORGANISATIONS
POTENTIAL BENEFITS	• Customers receive additional support from firms, more tailored to their needs • Customers spend less time and effort disclosing information about their vulnerable situation • Minimises emotional impact of multiple disclosures	• Greater regulatory compliance • More sustainable arrangements reached with customers • Overall reduction in time-cost of calls for organisations • Improved customer satisfaction
POTENTIAL RISKS	• Poor-quality data is recorded & shared • Error in data use, interpretation, storage that creates detriment • Exclusion from the market or from extra support • Exploitation by unscrupulous firms • Exposure to frauds and scams	• General Data Protection Regulation (GDPR) non-compliance • Data breaches • Misuse of shared data • Costs of new systems and processes

Source: authors' summary of evidence and interviews with stakeholders

Executive Summary

Five building blocks for greater data-sharing

The evidence suggests there may be considerable benefits to data-sharing but also highlights risks that need to be managed correctly. Drawing on other sectors' experiences, to examine how such a system might work in practice we considered five building blocks for greater data-sharing (**see Part Three**):

1. **Data disclosure** – organisations first need to consider ways of encouraging consumers to proactively disclose information about vulnerable situations to them. Crucially this involves creating an environment in which the consumer is comfortable and explaining why this information may be required.
2. **Data capture** – vulnerability is often complex, multi-faceted and episodic, which makes it difficult to neatly categorise in the binary way usually favoured by digital systems. Firms therefore need to consider how to capture data in a standardised way, if data-sharing is to work.
3. **Data hygiene** – data-sharing requires the introduction of systems to ensure that data is error-free and up-to-date, especially where consumers are affected by short-term or episodic vulnerabilities.
4. **Data sharing** – here we present a number of different models of data-sharing and new technology that could enable such a system to work in practice.
5. **Data control** – regardless of the system used to share data, it is of fundamental importance that the consumer retains control over their data and is able to change or delete the information stored about them, as required.

1. Data disclosure

For data-sharing between organisations to be effective, consumers first need to disclose this information to the organisation or at least give their consent for existing data held about them to be disclosed by one organisation to another.

From our consumer survey, disclosure by consumers with mental health problems is not uncommon. Yet significant numbers of people do not disclose information about their mental health; and this may well apply to other vulnerable situations as well, such as substance addictions, gambling problems or domestic abuse. There already exist tools and protocols to help financial services staff deal appropriately with customer disclosure. Some of our industry experts felt that encouraging more customers to disclose information about their vulnerable situation to firms (and ideally to disclose it earlier) would be a useful first step towards greater data-sharing.

What's happening in other sectors? Working with the energy sector, Citizens Advice plans to create a universal and accessible online registration process for the Priority Services Register (PRS) to make it easier for energy customers to apply for non-financial support services.

In the gambling industry, people can ask to be self-excluded from all Licensed Betting Offices that they use or are likely to use, under the Multi-Operator Self-Exclusion Scheme (MOSES) – although the scheme's effectiveness has been questioned.

Executive Summary

2. *Data capture*

Financial services firms have well-established systems and processes for capturing customers' financial transaction data and sharing it e.g. with credit reference agencies. Capturing data about someone's (non-financial) vulnerable situation is a very different prospect and one that provoked a lot of discussion in our expert interviews.

Defining vulnerability from an operational perspective was seen as a vital first step towards greater data-sharing, but one that is challenging not least because of the wide spectrum of different vulnerable situations and the various degrees to which they may affect individuals. Under GDPR, the collection of personal data should also be "limited to what is necessary", rather than "not excessive" (as in the Data Protection Act).

One solution might be a standard classification of vulnerability that provides more information than a simple vulnerable/not vulnerable flag and can help firms decide their own intervention or 'treatment' strategy. Even if a standard classification does not completely negate the need for further contact with a customer, it might assist a more outcomes-focused conversation. It was clear from our research that any new plans for greater data capture and data sharing would have to work within the constraints of organisations' existing information systems.

What's happening in other sectors? The energy sector has worked through similar issues regarding vulnerability definitions and classifications. An industry-led group has, over the last two years or so, worked together to develop a set of standardised vulnerability Needs Codes (the categories that allow customers to register on the Priority Services Register for additional support) that are being rolled out across electricity and gas companies. The Needs Codes cover particular circumstances and conditions (e.g. people who are dependent on medical equipment, or who have poor mobility, communication difficulties or mental health problems), which are perhaps more prescriptive than the wider understanding of vulnerability that exists in financial services.

3. *Data hygiene*

Data hygiene means making sure that data is relatively error-free. For personal information about vulnerability, our expert interviewees focused in particular on the importance of maintaining accurate and up-to-date data in the interests of customers, and in line with data protection law.

For relatively stable long-term circumstances or situations, this may be fairly straightforward. However, a vulnerable situation might well be episodic or transitory which makes data hygiene more challenging. In these situations, how can organisations maintain accurate data (including removing data if customer consent is withdrawn)? One way is an outbound customer contact programme run by the organisation that holds the data. For individual firms to run their own customer contact programmes could be costly and duplicative, and almost inevitably involves a time lag between the customer disclosing new information and their records being updated. On the other hand, if they rely on inbound customer communication, firms' may well end up with out-of-date vulnerability data.

Executive Summary

What's happening in other sectors? In the energy sector, there are temporary Needs Codes (such as post-hospital recovery) that enable customers to join the Priority Services Register for non-financial support. According to our expert interviews, energy companies are expected to update and clean their register data periodically. For temporary Needs Codes, this might involve contacting the customer to check their situation; expiring the data according to a pre-agreed time period; or leaving the code in place until the customer contacts their supplier in the normal course of business.

4. Data-sharing

Most private and third sector organisations already have a general ability to share information, provided this does not breach data protection or any other law. We looked in detail at three possible models for organisations to share more data about customers in vulnerable situations. Any data-sharing model can only be as good as the information that organisations record, however, and their systems for data collection, use, storage and sharing.

Model 1: Company-to-company sharing. Company A receives information from a customer about their vulnerable situation and shares this with other firms as agreed with the individual and in line with data protection law. An example of this data sharing model is the Priority Services Register that operates in the energy industry.

Model 2: Customer-facing vulnerability register. An individual in a vulnerable situation adds their details to a third-party database (or someone with Power of Attorney does it for them). Companies either search this database or are automatically updated about the customer's situation, in line with data protection law. An example of this data sharing model is the Vulnerability Registration Service.

Model 3: Third-party inter-company database. Company A receives information from a customer about their vulnerable situation and shares this with a third-party database provider, in line with data protection law. Other companies can be notified if one of their customers is added to this database or they can search the database themselves. An example of this data sharing model is a credit reference agency.

Another option might be for individuals to share vulnerability information via the Notice of Correction system operated by credit reference agencies (where individuals can add a note to their credit file if they want to provide an explanation or feel something is misleading). However, in their current form NOCs may not provide an optimal way of recording and sharing vulnerability data for data capture and data hygiene reasons.

A different approach might be to use blockchain technology. Blockchain is an encoded digital ledger that is stored on multiple computers in a network that exists without a centralized authority or server managing it. This new technology could offer another way for individuals and organisations to securely share personal data - and allow individuals close control over the ways in which their data are shared and used. For example, at any given time an individual may alter the set of permissions for their data and revoke access to previously collected (or shared) data.

Executive Summary

5. Data control

The preceding building blocks have mainly considered data control from an organisational perspective. But what about personal control over data-sharing and data use? In a 2011 publication, the World Economic Forum noted the emergence of personal data services which "… *provide the safe means by which an end user can store, manage, share and gain benefit from his or her personal data*."

With a personal data service, an individual's identity is validated and assured, reducing the risk of fraud for the end-user and the organisations that they share data with. It can also simplify data management, for example by doing away with the need for multiple passwords.

An example of a personal data service in the UK is Mydex, a Community Interest Company. Mydex users can choose what data they want to store and potentially share. They can also create their own set of verified proofs about their situation (e.g. their identity) and store a verified copy of the data which they share and manage themselves.

Among our expert interviewees, there was also interest in the opportunities that Open Banking might offer to help people manage their own data – initially financial transaction data, but potentially also vulnerability data. An individual might, for instance, be able to give an aggregator service access to their data, that could then be on-shared with other organisations as determined by the customer, for example via a data dashboard where they could switch access to their data on or off.

This, of course, raises a practical question about whether customers in vulnerable situations are always able to exercise 'data control' in their lives, due to their vulnerable situation making it more difficult.

Steps towards greater data-sharing

While certainly challenging, our expert interviewees did not want to relegate vulnerability data-sharing to the 'too difficult pile'. So what are the next steps towards greater data-sharing among financial services organisations? Our research suggests three possible steps:

- For firms to look at ways to achieve better data-sharing *within* their own organisation or corporate groups – a significant issue, according to our expert interviews.
- To undertake proof of concept work; for example, pilots to share data for one type of vulnerability, such as one or more long-term health conditions or disabilities.
- To explore the feasibility of a shared way of classifying vulnerability.

If individuals or organisations want to take these (or other) steps forward, we believe our research findings offer a useful starting point.

The data-sharing debate is still at an early stage. As GDPR comes into force and technology continues to advance (bringing down the costs of infrastructure changes), we should see more opportunities for data to be used as a force for good, for the benefit of consumers and firms.

About this research

About this research

This report asks whether greater sharing of data between financial firms can improve their ability to identify and support customers in vulnerable situations.

Every day, hundreds, if not thousands, of people face really tough conversations with their financial services providers. They might need to disclose the death of a loved one, or reveal that they are living with a serious mental health condition which is severely affecting their finances. For many people, sharing such information is draining – no matter how kind, polite and empathetic the person at the other end of the phone line is. After putting the phone down, the last thing that most people will want to do is to repeat the conversation with one another firm, and then probably another one after that.

It is possible that sharing data about these situations could be much easier. Rather than having multiple, similar conversations with different firms – which can be difficult and time-consuming – what if the first firm that an individual speaks to could simply notify all the others that they need to deal with? This would ensure that all firms that the customer deals with are in a better position to support them with whatever they are going through.

In a world of often near-instantaneous data transfer, greater data-sharing between financial services firms of non-financial data is theoretically possible but there are many issues to consider, from the practicalities and costs to the question of what data – if any – consumers feel comfortable to share.

With a grant from Barrow Cadbury Trust, we carried out independent research to shed light on data-sharing between organisations, an area that has received relatively little attention to date. While our focus is sharing data about vulnerable situations, many of the lessons from the research could apply to data-sharing generally; and to data-sharing *within* organisations as well *between* organisations. Rather than recommending a definitive solution or offering the 'final word' on data-sharing, our aim is to provide a solid basis for further meaningful discussion about this complex issue.

Disclosing personal information can be draining – whether it's about a health issue, a bereavement or some other difficult situation.

Rather than having multiple, similar conversations with different firms, what if the first firm that an individual speaks to could simply notify all the others?

About this research

Our research comprised a thorough review of the available evidence; an online survey of people with mental health problems; and in-depth expert interviews with representatives from financial services, the energy and water sectors, the advice sector, and data specialists.

To investigate data-sharing between organisations (and financial services firms in particular), we started by reviewing available evidence, looking at different data-sharing models and considering the legal and regulatory frameworks in which data-sharing occurs. We reviewed around 120 pieces of evidence from different sectors, including financial services, health, utilities, and government services. The evidence we reviewed took the form of academic peer-reviewed articles and papers; research reports and information produced by UK government, regulators, think-tanks, non-profit and for-profit organisations; regulations and guidance relevant to data-sharing and vulnerability; and international evidence from organisations such as the World Economic Forum and the European Commission.

We then consulted experts to find out more about the data-sharing that already occurs, the appetite for greater sharing and what steps would be required to make it happen. To get the perspective of experts-by-experience, we conducted a short online survey with members of the Money and Mental Health Policy Institute's Research Panel, who all had first-hand experience of mental health problems. We received 244 responses to the survey.

To get the perspective of industry and consumer experts, we carried out telephone interviews with 18 organisations, selected to include financial services firms and trade associations, data specialists, representatives from the energy and water sectors, and representatives from the advice sector. Some of these experts had participated in our previous research on vulnerability; others came to our attention through the evidence review; or were recommended. The interviews took place between September and December 2017.

By opening up this complex area to scrutiny, this study surfaces the key issues and challenges that firms and regulators need to consider in terms of data-sharing between organisations, including options for giving individuals control over the type and amount of data that is shared.

Part One:
What’s the context for this research?

Collecting data from individuals – current practice

There is limited publicly-available documentation that outlines precisely how different organisations handle data about vulnerability when it is disclosed to them by a customer (or their representative). From our own research, it appears that the TEXAS protocol (Figure 1) is often used by creditors and debt collectors to manage and record the disclosure of a vulnerable situation.[1]

Once a customer has been informed how their data will be used and has given their consent for the data to be recorded, organisations must ensure they have a robust, accurate and secure way of storing and using this data. Organisations may operate a system of 'flags' or 'markers' on the customer's account that indicate some form of vulnerability. The flags vary from organisation to organisation: while some might use a relatively simple 'binary' flag, where the account either has a vulnerability attached to it or not, others might have a more complex system with flags that indicate type or severity of situation or how the situation may affect the customer's management of their account. Alongside the flag, staff may also have a facility to record more detailed notes about the customer and their situation. Crucially, in line with the third principle of the Data Protection Act, such notes should be 'adequate, relevant and not excessive'.

There is guidance on the handling of sensitive personal data by creditor organisations, produced through a collaboration between the Money Advice Liaison Group and Royal College of Psychiatrists.[2] This guidance recognises the difficulties that creditors face in relation to customers in vulnerable situations (in this case mental health), and sets out how such information should be collected, recorded, and stored. While the guidance makes some reference to information-sharing between organisations, it is partial and incomplete.

Figure 1 – the TEXAS Protocol (based on Fitch, Evans & Trend, 2017)

T	**T**hank the customer (what they have told you could be useful for everyone involved).
E	**E**xplain how the information will be used (it is a legal requirement). This explanation should include why the information is being collected, how it will be used to help decision making, and who the data will be shared with/disclosed to.
X	e**X**plicit consent should be obtained to record this information (it is a legal requirement).
A	**A**sk the customer questions to get key information (these will help you understand the situation better), e.g. how situation affects ability to manage finances and communicate with creditors.
S	**S**ign-post or refer to internal and external help (where this is appropriate)

The regulatory context

Sharing data about customers in vulnerable situations is a complex area of policy and practice because it spans financial services regulation – which mainly sits with the Financial Conduct Authority (FCA) – and data protection – which is regulated by the Information Commissioner's Office (ICO).

Financial services regulation

The FCA's overall approach is to give vulnerable consumers greater levels of consumer protection.[3] Its high-level Principles for Business that are relevant to vulnerability include Principles 6 (customers' interests) and 7 (communications with clients) – set out in full in Box 1. While the FCA may use these Principles to guide its supervision and enforcement, there are also specific rules in its Handbook that relate to vulnerable customers: in the conduct standards for lending, debt collection and arrears, and in the conduct standards for debt advice.

Data protection

When handling customer data, organisations must comply with all relevant legislation regarding the collection, processing, storing and sharing of this information. For organisations operating in the UK, this has primarily been the Data Protection Act (1998).[4] The Data Protection Act (DPA) defines what 'data' is and what constitutes 'personal' and 'sensitive' data (e.g. personal data about a person's physical mental health or condition). The ICO is responsible for enforcing the DPA. From May 2018, the DPA will be replaced by the EU-wide General Data Protection Regulation (GDPR).

Box 1 - FCA Principles for Business relevant to sharing data about customers in vulnerable situations

Principle 6: A firm must pay due regard to the interests of its customers and treat them fairly.

Principle 7: A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.

EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) largely replicates the Principles of the DPA, though there are a number of changes which financial organisations need to consider – in relation to the way they handle data both on vulnerable customers and on customers more generally.[5]

From May 2018, organisations must request individuals' consent to record information in a clear and easy to understand format, rather than hidden in terms and conditions; the purpose of data processing should be attached to that consent. While this may impact how organisations obtain consent from customers at account opening, in theory it should have limited impact on the way organisations obtain consent from customers to record information about a vulnerable situation – because this consent should already be obtained in a

The regulatory context

transparent way, usually over the course of a telephone conversation with the individual.

One change with potentially more significant ramifications is that collected personal data should now be “limited to what is necessary”, rather than “not excessive” (as in the DPA). An organisation must therefore demonstrate that any data recorded about a vulnerable individual is entirely necessary to fulfil their regulatory obligations to treat vulnerable customers fairly. This may require clearer guidance from firms to their staff about what information is essential and what is not.

Finally, GDPR introduces higher penalties for organisations that breach GDPR: for the most serious breaches, organisations may be fined up to 4 per cent of their annual global turnover or €20 million (whichever is higher); for lesser breaches they could be fined 2 per cent of their annual global turnover or €10 million.

Part Two:

What's the case for greater data-sharing between organisations?

What's the case for data-sharing between organisations?

When exploring the viability of any intervention we should first ask ourselves: is there a need for it? In this section we therefore consider whether a sufficient need exists for greater sharing of data between organisations about consumers in vulnerable situations.

To do this, we ask and attempt to answer the following questions:

- How often are (and aren't) consumers disclosing information about vulnerable situations to organisations?
- What are the possible benefits and risks to *consumers* as a result of data-sharing between organisations?
- What are the possible benefits and risks to *organisations* as a result of sharing data with one another?

Throughout this section we draw heavily on our survey of individuals with lived experience of mental health problems, as well as wider literature and our interviews with industry experts and other stakeholders.

Ways to assess the need for greater data-sharing:

- ***Current levels of customer disclosure***
- ***Benefits and risks to consumers***
- ***Benefits and risks to organisations***

How common are disclosures of vulnerable situations?

In order to ascertain whether a need exists for data-sharing arrangements between organisations, the obvious starting point is to consider how many consumers are already disclosing vulnerable situations to organisations and how often consumers might be disclosing such situations to multiple organisations.

To understand how often consumers disclose such situations, we use data collected from frontline financial services staff in a previous study[6], as well as self-reported disclosures from consumers themselves. Financial services organisations also hold data on the number of customers that they have flagged as vulnerable (with the customer's consent), but little of this evidence is currently publicly available, primarily due to commercial implications.

Disclosures made to financial services staff

In 2017, the Personal Finance Research Centre published the results of a UK-wide survey of frontline staff working in the debt collection industry. The survey, which involved 1,573 individual debt collection staff working in 27 different firms, showed the extent to which staff members speak to customers (and third parties) who disclose information about various situations that may make them vulnerable, as shown in Table 1.

While these figures rely on staff members' recollection of such conversations and are therefore not as precise as organisations' internal system data (where this is collected), they nevertheless highlight the scale of the challenges facing staff when it comes to dealing with customers in vulnerable situations. For mental health problems, serious physical illness and bereavement the figures presented are all for individual members of staff. When these are scaled up to department- or organisation-level, it becomes clear that debt collection staff deal with a very large number of customer disclosures every month.

Table 1 - Frequency of disclosures to debt collection staff[7]

Mental health problems	Median of **12** disclosures to each member of staff per month
Serious physical illness	Median of **15** disclosures to each member of staff per month
Bereavement	Median of **9** disclosures to each member of staff per month
Customers at risk of suicide	**1 in 4** frontline staff spoke to at least one customer they seriously believed might kill themselves in the last 12 months
Terminal illness	**3 in 4** frontline staff received a disclosure about a customer diagnosed with a terminal illness in the last 12 months

How common are disclosures of vulnerable situations?

Disclosures reported by consumers with mental health problems

The consumer survey conducted for this study also shows that it is not uncommon for people with mental health problems to disclose this information to the organisations they come into contact with.

Table 2 shows that 44 per cent of our survey respondents had disclosed information about their mental health problem to at least one bank and 38 per cent had disclosed this to other lenders, such as credit card or personal loan companies.[8] This indicates that disclosure is reasonably common. It is important to acknowledge that, as the respondents self-selected into the Money and Mental Health Policy Institute's research community, they may be more aware of organisations' support for people with mental health problems than the 'general population' of people with such conditions and therefore possibly more likely to disclose their mental health problem.

A larger proportion of our survey respondents meanwhile had disclosed this information to Government agencies, such as DWP or their local authority (88 per cent), and organisations that provide advice about money or debt problems (63 per cent). Neither of these statistics are particularly surprising given Government agencies' role in assessing eligibility for sickness and disability benefits, and given advice organisations' role in supporting individuals to maximise their income, which requires them to understand their clients' potential eligibility for such benefits.

Table 2 - Percentage of respondents who had disclosed information about their mental health problem to at least one of the following types of organisation

88 per cent	had disclosed to **government agencies**
63 per cent	had disclosed to **money/debt advice organisations**
44 per cent	had disclosed to **banks**
38 per cent	had disclosed to **other lenders**
32 per cent	had disclosed to **utilities providers**
30 per cent	had disclosed to **insurance companies**
11 per cent	had disclosed to **telecoms organisations**
66 per cent	had disclosed to **at least one of the above**

How common are disclosures of vulnerable situations?

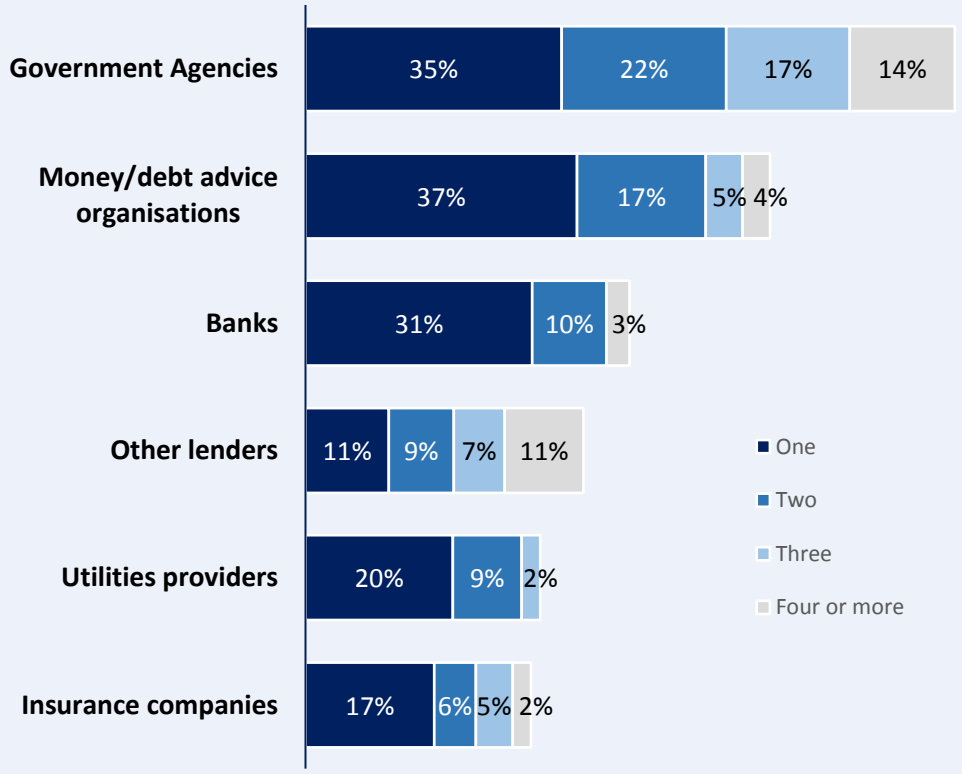
Do consumers disclose to multiple organisations?

We also asked our survey respondents to tell us how many of each different type of organisation they had told about their mental health problem, the results of which are given in Figure 2.

This shows that over half of respondents (53 per cent) had disclosed their condition to two or more different Government agencies, a quarter had done so for two or more advice organisations (26 per cent), as had a similar proportion for two or more other lenders (26 per cent), and nearly one-in-seven had told two or more banks (13 per cent).

On the one hand, this suggests that when an individual discloses their mental health problem to one organisation, it is quite likely that they will also disclose their condition to other organisations as well. On the other hand, it also shows that there are still a considerable number of people who only disclose their condition to one organisation. One possible explanation is that some people only come into contact with one organisation of this type. But for others who do deal with more than one such organisation, are there other factors that lead them not to disclose?

Figure 2 - How many of each type of organisation have consumers told about their mental health problem? (% of all respondents)



How common are disclosures of vulnerable situations?

How many people with mental health problems are not disclosing information about their condition to organisations?

In order to better understand consumers' disclosure behaviour it is important to also consider those people who choose not to disclose their condition to any or all organisations they deal with.

We find that a considerable proportion of consumers do not disclose information about their situation to creditors or other organisations. As shown in Table 3, nearly a third (31 per cent) of consumers had not disclosed information about their mental health problem to any of the types of organisation asked about in our survey. When looking solely at financial firms, as many as 56 per cent had not disclosed their condition to their bank(s) and 62 per cent hadn't disclosed to any other type of lender.

Respondents who had not disclosed to any of these organisations were asked why this was the case, in a question adapted from a survey carried out in 2011 by the mental health charity Mind that focused on people's experiences of dealing with their creditors.[9] Table 4, on the following page, sets out the findings from the 2011 Mind survey and our 2017 consumer survey (which asked about creditors and other organisations). As the two surveys were carried out with different convenience samples[10], they are not strictly comparable. However, they do suggest there have been some changes to the reasons for non-disclosure over time among people with mental health problems.

Table 3 - Percentage of respondents who had not disclosed information about their mental health problem to one or more of the following types of organisation

89 per cent	hadn't disclosed to **telecoms organisations**
70 per cent	hadn't disclosed to **insurance companies**
68 per cent	hadn't disclosed to **utilities providers**
63 per cent	hadn't disclosed to **other lenders**
56 per cent	hadn't disclosed to **banks**
37 per cent	hadn't disclosed to **money/debt advice agencies**
12 per cent	hadn't disclosed to **government agencies**
31 per cent	hadn't disclosed to **any of the above organisations**

How common are disclosures of vulnerable situations?

Table 4 - Reasons given for not disclosing their mental health problem to any listed organisation (% of those who had not disclosed to any listed organisation)

Reason for not disclosing:	2011 (Mind)	2017 (PFRC)
I wasn't aware that it would make any difference to how the organisation dealt with me / the debt	70%	64%
I do not like telling people about my mental health problems	65%	48%
I was concerned about what they would do with the information about my mental health problem	64%	47%
I thought I would be treated unfairly if I did	54%	44%
I did not believe they would understand my mental health problem	73%	41%
I was worried that it would stop me accessing certain products or services in future	49%	39%
I did not think I would be believed	53%	16%
Other	4%	8%
I haven't come into contact with any of these types of organisation	7%	3%

It is interesting to note the apparent continued lack of awareness among consumers about why organisations might need information about a consumer's mental health: 64 per cent of respondents in 2017 said that they did not disclose because they were not aware that it would any difference to how the organisation dealt with them.

The second most common reason for not disclosing was that respondents do not like telling people about their mental health problem (48 per cent in 2017). Encouragingly, this number is 17 percentage points less than reported in 2011 (although this might have something to do with the different survey populations). In a similar vein, fewer respondents in 2017 said they did not think the organisations

How common are disclosures of vulnerable situations?

would understand their mental health problem (41 per cent) or that they thought they would not be believed (16 per cent).

There appears to be some concern about what organisations would do with any information that is disclosed; this was given as a reason for non-disclosure by 47 per cent of respondents. This of course is highly relevant to the data-sharing question, and suggests that organisations need to be very clear with consumers precisely what will happen to any information they disclose, possibly before they have even disclosed it at all.

The last significant concern raised by the survey relates to people's fears about being excluded from products and services. Four in 10 respondents in our 2017 survey (39 per cent) were worried that disclosing information about their mental health problem would stop them accessing products and services in the future. This is particularly relevant to accessing credit products but the Money and Mental Health Policy Institute has also identified potential issues in the insurance market around the fair treatment of consumers with mental health problems.[11]

All of these explanations for a lack of disclosure are understandable given the highly personal nature of data about an individual's mental health, especially when combined with equally sensitive data in relation to someone's financial circumstances. Indeed, we asked our survey respondents to rate how personal they found different types of information about them on a scale from one to ten, where one is 'very personal' and ten is 'not at all personal'. Table 5 shows the percentage of respondents who rated each piece of information between one and three out of ten. Unsurprisingly this confirms that both money and mental health are extremely personal topics for these individuals.

Table 5 - Percentage of respondents who describe each of the following pieces of information as very personal (rated between one and three on a one-to-ten scale, where one is 'very personal') (% of all respondents)

Your financial situation	**86 per cent**
Information about your mental health	**82 per cent**
Your telephone number	**75 per cent**
Information about other aspects of your health	**75 per cent**
The places you visit frequently	**52 per cent**
Your email address	**42 per cent**
Your favourite websites	**40 per cent**
Your gender	**11 per cent**

How could data-sharing benefit consumers?

In this section we consider the possible benefits to consumers of organisations sharing data with one another about their vulnerable situation.

There are three main ways in which such a system might provide benefits to consumers in vulnerable situations:

- Ensuring that consumers in vulnerable situations receive **adequate support** for their circumstances.
- Reducing the amount of **time** that individuals have to spend disclosing information to multiple organisations.
- Minimising the **emotional impact** of disclosing information about difficult circumstances to different organisations.

We consider each of these in turn.

Possible benefit 1: Ensuring that consumers in vulnerable situations receive adequate support

As our research has shown, there are considerable numbers of individuals who are not disclosing information about their situation to various organisations. There are possibly also a considerable number of individuals who are disclosing their situation to only one organisation and not to others that they come into contact with. This may mean they miss out on additional support or helpful adjustments that organisations could make. Such adjustments might include:

- Providing information in an alternative format, e.g. large font, Braille, sign language.
- Giving consumers a greater choice over the channel used to contact them (e.g. telephone, email, letters), as well as the best time to contact them.
- Making reasonable adjustments in relation to the repayment of debts, such as allowing individuals to schedule payments in a manner more suitable to their individual circumstances.
- Allowing consumers to block certain 'merchant codes' or categories of spending, e.g. at gambling outlets, or late night spending.

With increased data-sharing between organisations, consumers would only need to disclose information about their situation to one organisation in order to benefit from this support from all of the organisations where they hold an account.

How could data-sharing benefit consumers?

Possible benefit 2: Reducing the amount of time that individuals are required to spend disclosing information to multiple organisations

As evidenced by the below quotes from our 2017 survey respondents, the process of disclosing information to organisations about certain health conditions or other vulnerable situations can take a considerable amount of time:

> *"I suffer from Huntington's disease a neurological condition which leaves me very isolated and can suffer depression... Try telling someone by telephone and they are not interested even though I need more time to talk and communicate and more time to understand someone who talks very quickly on the telephone. [I prefer] people who work in an organisation or role which is trained to understand and help and allow more time for your disability."* (Consumer survey respondent)

> *"My bank constantly wrote to me asking to complete long forms and budget planners. Put me off bothering to complete them… [My phone company] allowed me to end my contract as I told them I'd taken it out when manic. However the whole process took months with much chasing up."* (Consumer survey respondent)

The process of obtaining and sharing sufficient medical evidence is also time-consuming, as shown below. While data-sharing wouldn't necessarily speed-up the process of obtaining evidence, it could mean that consumers might not be required to spend time sharing documents with multiple, individual organisations.

> *"In regard to Government departments, I informed them in applications for certain benefits (DLA, disability element of housing benefit, disability element of tax credits)… The difficult part was providing necessary evidence - letters from Doctors and counsellors were required, and these were not necessarily available due to the time needed to wait for appointments, etc."* (Consumer survey respondent)

By removing the need for individuals to disclose the same information multiple times, there could be a real time-saving element for consumers (and organisations, as we touch on later). This, it could be argued, is likely to improve consumer satisfaction with the service they receive and may also result in better consumer outcomes if people receive help sooner.

How could data-sharing benefit consumers?

Possible benefit 3: Minimising the emotional impact of disclosing information about difficult circumstances to different organisations

Our 2017 consumer survey respondents who had disclosed information about their mental health to at least one organisation were asked how easy or difficult they found disclosure.

As displayed in Table 6, more than two-thirds (67 per cent) of those who had disclosed their mental health problem to a bank reported that they found it difficult to do so. 'Other lenders' fare only slightly better, with 65 per cent of respondents finding it difficult. Government agencies were also a particular source of difficulty for 62 per cent of consumers, which is perhaps worrying given that more consumers reported disclosing their mental health problem to government agencies than to any other type of organisation.

We asked respondents why they found it difficult to disclose to organisations. The most common responses were as follows:

- Feelings of shame or the fear of being judged (27 per cent)
- Find it difficult to talk about mental health because it is a private subject (19 per cent)
- Disclosures to the DWP were particularly difficult (16 per cent)
- The organisation's processes or procedures made disclosing more difficult (16 per cent)
- The organisation put them under pressure to talk about their mental health (2 per cent)

Table 6 - Percentage of respondents who found it 'very' or 'quite difficult' to disclose information about their mental health problem to each of the following types of organisation

Banks	**67 per cent**
Other lenders	**65 per cent**
Government agencies	**62 per cent**
Telecoms organisations	**50 per cent**
Utilities providers	**46 per cent**
Insurance companies	**39 per cent**
Money/debt advice organisations	**34 per cent**

Percentages include only those who had disclosed information about their mental health problem to at least one organisation of this type.

How could data-sharing benefit consumers?

Their responses highlight the clear emotional strain that such disclosures can place on consumers:

> *“Having to explain to banks/ other people you don't know but you are forced to explain is very stressful and unnerving and also embarrassing and can add to your negative emotions - I find after I have had to have this discussion I come away feeling guilty and angry with my past (even though it's not my fault I'm ill). I beat myself up at my lowest point I felt so inadequate that it made me feel suicidal.”* (Consumer survey respondent)

> *"When I'm struggling I find it very difficult to deal with anyone - whether face to face or on the phone. I can manage email or forms just about, but often this isn't an option. I'm expected to talk to people when it's the last thing I'm able to do."* (Consumer survey respondent)

> *“I sat and cried in an open office with strangers all around because they were asking me questions about how my severe depression and anxiety prevented me from seeking work - not exactly empathetic or understanding of the situation and no clue how to handle me, my responses and how upset I was.”* (Consumer survey respondent)

Given that data-sharing could reduce the number of times an individual has to disclose information about their situation and the amount of time they have to spend doing so, it could also reduce the emotional strain associated with disclosure. For individuals with mental health problems this could be a significant benefit, but the same could also be true for individuals in other vulnerable situations, for example, those going through bereavement.

What are the risks to consumers of greater data-sharing?

Having considered the possible benefits to consumers of increased data-sharing, it is necessary to also consider the risks associated with any changes to the current system.

Here we consider the following five areas of risk:

- Poor-quality information
- Error
- Exclusion
- Exploitation
- Exposure

Our expert interviews confirmed these to be the main risks to consumers, with potential for greater detriment where people are in vulnerable situations. Any new models of data-sharing would need to manage these risks appropriately.

Possible risk 1: Poor-quality information

One of the key risks to consumers is that the information recorded and shared by one organisation is not sufficiently clear, consistent or detailed to be useful to another organisation. This might result in false positives (someone is flagged as vulnerable when they are not) or false negatives (someone is not flagged as vulnerable when they are).

It could also lead to other organisations misinterpreting the support needs of the consumer and may mean that consumers are required to re-explain their situation to each organisation. Such a requirement would therefore largely remove any benefits in terms of the time and effort needed to disclose.

Possible risk 2: Error

Data protection law aims to ensure proper treatment of data by any organisation that holds that data. Nonetheless, there is a risk of error in the use, interpretation and storage of data that could create consumer detriment. The more organisations the data is shared with, the less able are consumers to check their data is used and store appropriately by those individual firms. One answer could be a common standard for data-sharing that firms sign up to, or building on any existing standards for data-sharing e.g. governing how firms share data with Credit Reference Agencies (CRAs).

Possible risk 3: Exclusion

Organisations could use such information to restrict consumers' access to different services or products, which might lead to exclusion from the market.

> *"… there's the worry that if you are on that list, are you going to be essentially blacklisting yourself forever, how long is that going to stay on there, what can people use it for?"* (Expert interview, financial services)

Organisations should, however, specify how they (and other organisations) will use the information provided by the consumer and if they were to use the information for purposes other than those

What are the risks to consumers of greater data-sharing?

specified it could certainly be argued that they are in breach of data protection regulation.

There is also a different risk of exclusion: if organisations rely too heavily on one source of information (such as a single database) to flag that someone is in a vulnerable situation, then anyone not included in that source of information may not receive the help they need.

> *"… there may be some firms or some customers that just choose not to interact through that medium, so you wouldn't want like [company name] for example to say, Right we're only going to treat you as vulnerable if we see that you're vulnerable on this data storage.* (Expert interview, financial services)

Similarly, organisations may no longer feel that is their job to identify vulnerability if they can rely on a central database or another organisation to do it for them, potentially allowing vulnerable customers to go unnoticed.

Possible risk 4: Exploitation

Similar to the risk of exclusion described above, it is possible that unscrupulous firms could use shared data about vulnerability to exploit consumers. They could, for example, use the data to carry out aggressive marketing against consumers when they are at their most vulnerable. Again, however, such a move would likely breach data protection regulation, not to mention FCA-regulated firms' duty to ensure the "fair and appropriate treatment" of customers in vulnerable situations.[12]

Possible risk 5: Exposure

There is a risk that individuals in vulnerable situations are exposed to fraud and scams by virtue of sharing more data and the potentially long data chains that this could create. Evidence suggests that scams and fraud are high up on people's list of concerns, so this is something that needs to be addressed if data-sharing is to be accepted by consumers.[13] One way to tackle this is to ensure that the number of organisations that data is shared with is limited and bounded; for example, only those with certain FCA permissions.

What are the trade-offs for consumers?

Data-sharing is an issue about which the general public expresses strong views, but where information and power imbalances can make it difficult for individuals to objectively weigh up the pros and cons of sharing their data.

The evidence suggests that, in general, individuals are aware of trade-offs between the perceived risks of sharing their data with another party and the benefits they may derive as a result. Some of the commonly cited trade-offs are summarised in Table 7.

Table 7 - Commonly cited trade-offs in personal data sharing (source: authors' summary of evidence)

	Data exchange	Data use	Data control
What individuals think is fair	To receive some benefit from sharing data	For organisations to use the data only for the intended purpose to which they have agreed	To control how their data is used and shared
What individuals think is unfair	For their data to be used for unrelated, unilateral gain by the recipient organisation	For organisations to use the data for some other purpose without their permission For organisations to sell their data without their permission	For organisations to use the data for some other purpose without their permission For organisations to sell their data without their permission To be exposed to frauds and scams because of data collection and use

What are the trade-offs for consumers?

Fewer than two in ten (16 per cent) of our consumer survey respondents said they would not allow an organisation to share data about their mental health with another organisation under any circumstances. The other 84 per cent might be happy for organisations to share this data, under certain circumstances. As we see in Table 8, the top three circumstances were trust in the organisations that would share their data; the potential for a better service; and saving time and effort.

Table 8 – Reasons why respondents might allow an organisation to share data about their mental health with another organisation

71 per cent	If I **trusted both organisations** to handle this information sensitively
58 per cent	If it led to a **better service** or one **more tailored** to my needs
50 per cent	If it **saved me the time and effort** of discussing my mental health problem
39 per cent	If it **saved me money**
16 per cent	I **wouldn't allow this** under any circumstances
6 per cent	Other

When it comes to our behaviour, the extent to which we think about - or are concerned about - risks and trade-offs when faced with actually sharing our data is debatable. For example, while survey respondents regularly say they want more control over their data, in practice they may not be willing to invest much time in personal data management – particularly if the accompanying information is difficult to comprehend. In a 2015 Eurobarometer survey, 58% of internet users said they usually read privacy statements, but 24% said they did not fully understand what they were reading. Of those who didn't usually read privacy statements, 41% said it was sufficient for websites to have a policy, 27% believed the law would protect them and 24% said websites probably wouldn't honour them anyway.[14]

Information and power imbalances between individuals and organisations also challenge the idea that individuals can make effective trade-offs. For example, unless individuals have some sense of the value of their data, it may be difficult to judge 'fair exchange' for themselves. In addition, individuals may never realise their data has been misused by an organisation. And in some circumstances individuals may have to agree to share their data in order to access a product or service.

How could data-sharing benefit organisations?

In order to answer the question of whether there is a case for increased data-sharing, it's important to examine the possible benefits and costs to *organisations* – as well as consumers – of such a scheme.

In this section we therefore consider a number of ways in which organisations might benefit from greater sharing of data about consumers in vulnerable situations:

- Greater regulatory compliance.
- More sustainable arrangements reached with consumers.
- Overall reduction in time-cost of calls to organisations.
- Improved customer satisfaction.

As we see, these are largely the flip-side of the benefits to consumers themselves.

Possible benefit 1: Greater regulatory compliance

First, and arguably most important from an organisation's point of view, is that they will be better placed to meet their regulatory obligations to ensure the fair and appropriate treatment of consumers in vulnerable situations. This is because greater data-sharing should help them identify those most in need of additional support, who otherwise might not receive any extra help.

Possible benefit 2: More sustainable arrangements reached with consumers

It could be argued that by improving the identification of consumers in vulnerable situations, organisations will be able to reach sustainable arrangements with a greater number of people. This is especially likely in a debt collection environment, where a failure to acknowledge an individual's circumstances can lead to the individual withdrawing from the process: some consumers with mental health problems, for example, can find it very distressing to deal with their creditors over the telephone. Without knowledge of this, the organisation may attempt to phone the consumer multiple times to no avail, which is likely to both increase the organisational costs of collecting the debt as well as cause considerable distress to the consumer. If, however, they are aware of the consumer's condition they may choose an alternative channel to contact the consumer, which may lead to a quicker resolution for them and a better outcome for the consumer.

Possible benefit 3: Overall reduction in time-cost of calls to organisations

As discussed earlier, disclosing a vulnerable situation to an organisation can be quite a time-consuming activity. This is true for both the consumer and the organisation. Data-sharing could potentially improve this. Rather than having multiple long phone calls with each organisation, the consumer might have just one slightly longer phone call with the first organisation they disclose to and then a series of much shorter calls with all subsequent organisations in which they can discuss

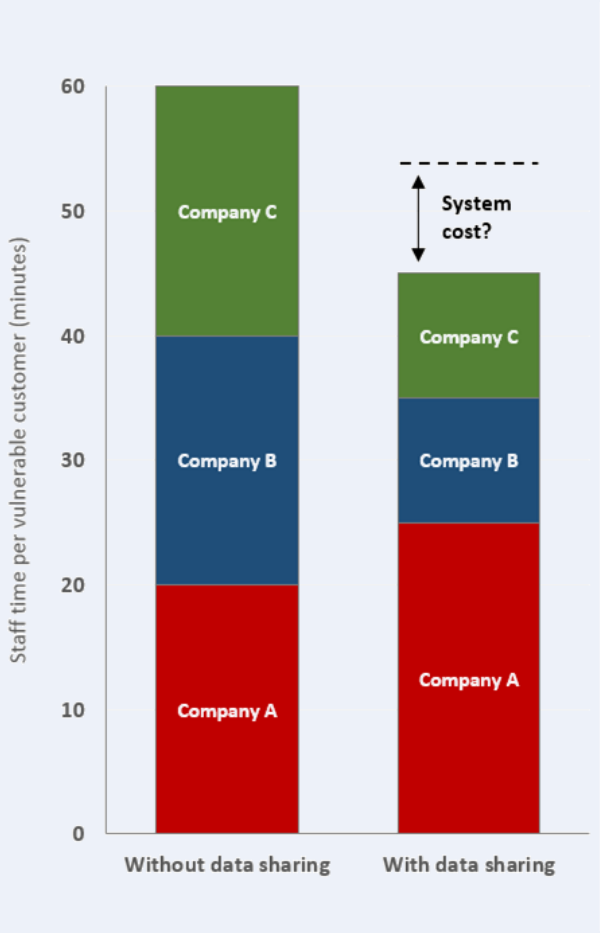
How could data-sharing benefit organisations?

the most appropriate course of action to take with that organisation. As shown in Figure 3, this could have an aggregate time-saving benefit across the organisations, though the unknown element is how the cost of any necessary changes to IT systems and infrastructure would impact upon the savings made. It is also worth noting that 'Company A' loses out somewhat in this system, though in reality the 'burden' of the first phone call would be more evenly distributed among the various organisations in the system.

Possible benefit 4: Improved customer satisfaction

The benefits to consumers in theory should lead to improved customer satisfaction, which may reduce complaints for organisations and improve staff morale. This could arguably increase staff retention, again providing organisations with further commercial benefit.

Figure 3 – Indicative example of potential time-saving for companies as a result of data-sharing.



A summary of potential risks and benefits

From our research, there broadly seems to be a case for greater data-sharing between firms - but with the caveat that the not insignificant risks are properly understood and managed.

In Table 9, on the following page, we summarise the benefits and risks of increased data-sharing, both for consumers and for firms. As can be seen from the table, many of the impacts for organisations are simply the reverse of those for consumers; for example, by minimising the amount of time that customers spend disclosing information to multiple organisations, firms also benefit from lower staff time costs in handling these disclosures.

Similarly, the risks to organisations are the flip-side of the risks to consumers: primarily, any misuse or mismanagement of data which has a negative impact on consumers is also likely to have negative impacts for organisations, mainly in terms of GDPR non-compliance and a substantial reputational and financial hit if they are caught.

The main unknown for firms is the cost and difficulty of implementing data-sharing with other firms. This is largely dependent on the precise system developed by firms and whether, for example, it makes use of existing IT infrastructure or requires new infrastructure. We consider these issues in Part Three, where we look at five 'building blocks' on which any model of sharing data should be based.

Data-sharing between firms about customers in vulnerable situations has the potential to be a force for good – provided the risks are properly understood, monitored and managed.

A summary of potential risks and benefits

Table 9 - Potential benefits and risks of data-sharing

	FOR INDIVIDUALS	FOR ORGANISATIONS
POTENTIAL BENEFITS	• Customers receive additional support from firms, more tailored to their needs • Customers spend less time and effort disclosing information about their vulnerable situation • Minimises emotional impact of multiple disclosures	• Greater regulatory compliance • More sustainable arrangements reached with customers • Overall reduction in time-cost of calls for organisations • Improve customer satisfaction
POTENTIAL RISKS	• Poor-quality data is recorded & shared • Error in data use, interpretation, storage that creates detriment • Exclusion from the market or from extra support • Exploitation by unscrupulous firms • Exposure to frauds and scams	• GDPR non-compliance • Data breaches • Misuse of shared data • Costs of new systems and processes

Source: authors' summary of evidence and interviews with stakeholders

Part Three:

A blueprint for data-sharing between organisations

A blueprint for data-sharing between organisations

Parts one and two set out the context for greater data-sharing between organisations. The evidence shows some considerable potential benefits for individuals and organisations, provided the not insignificant risks for people in vulnerable situations are properly understood, monitored and managed.

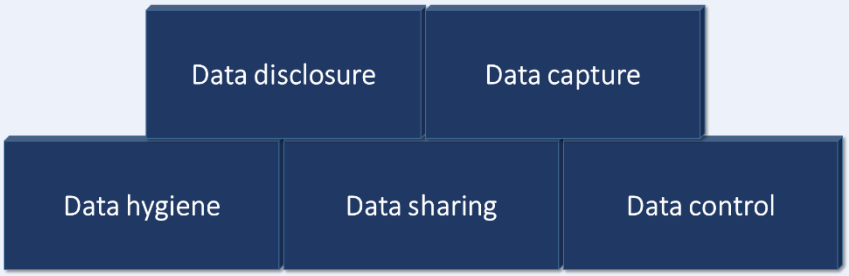
While not a perfect comparison, the consumer survey data from Mind in 2011 and for this study in 2017 seems to suggest that people may be more receptive now to sharing data about their mental health problems than they were in the past – although there remains a fair degree of scepticism and worry.

From the expert interviews we carried out for this study, it was clear that financial services firms are interested to explore greater data-sharing between organisations, and interested in learning from the experience of other sectors. While there has been some innovation in data-sharing in financial services, there remains fundamental questions about how data-sharing might work in practice. The industry is also understandably nervous about sharing sensitive personal data about an individual's vulnerable situation, particularly given changes to data protection law.

> *"… data-sharing for vulnerable customers does come up [at conferences]. So there is discussion, I think there's probably an element of nervousness around how that could be presented and accessed and controlled really."* (Expert interview, financial services)

In the following sections, we use the data from our evidence review and expert interviews to set out a blueprint for data-sharing between organisations. The blueprint is organised around five building blocks: data disclosure; data capture; data-sharing; data hygiene; and data control (Figure 4). In setting out this blueprint, we work through some of the thorny questions about how data-sharing might work in practice and explore what's happening in other sectors.

Figure 4 – Five building blocks to facilitate greater data-sharing



Building block I – data disclosure

For data-sharing between organisations to be effective, consumers first need to disclose this information to the organisation or at least give their consent for existing data held about them to be disclosed by one organisation to another.

As we saw earlier, disclosure among consumers with mental health problems is not uncommon: 44 per cent of our survey respondents had disclosed information about their mental health problem to at least one bank and 38 per cent had disclosed this to other lenders, such as credit card or personal loan companies. Yet significant numbers of people do not disclose information about their mental health; and this may well apply to other vulnerable situations as well, such as substance addictions, gambling problems or domestic abuse.

There already exist tools and protocols to help financial services staff deal appropriately with customer disclosure, such as the TEXAS protocol described in Part One. Some of our industry experts felt that encouraging more customers to disclose information about their vulnerable situation to firms (and ideally to disclose it earlier) would be a useful step towards greater data-sharing.

> "*…I just wonder if there is something around prompting, nudging customers to feel part of the application process, not in a detrimental way but there is the ability to share information about their circumstances*." (Expert interview, financial services)

The consumer survey data also gives us a good sense of what needs to happen for people in vulnerable situations to feel able and comfortable to share information about their particular circumstances. In particular, it would be important for them to understand the benefits of disclosing this information; the benefits of that data being shared with other organisations; and to have reassurance that they (and their data) will be treated fairly as a result of the disclosures.

What's happening in other sectors: Energy and water

In the energy and water sectors, work is ongoing to make better use of data-sharing to identify customers in vulnerable situations who could benefit from statutory non-financial support services, such as a large print bill or support to read their meter. This is a voluntary initiative supported by the energy and water regulators.[15] We talk more about this initiative later on.

In its work with energy and water companies, the UK Regulators Network (UKRN)[16] highlights the importance of demonstrating consumer benefit in order to build confidence in the data-sharing process and encourage disclosure:

> *"Customers should receive value from their data being shared, through a more tailored service or a better understanding of their needs. Customers that understand how they benefit from data-sharing will have more confidence in the process."* (UKRN 2017, page 11)

Building block I – data disclosure

In the energy sector alone, of the 11 million UK households eligible for the Priority Services Register (PSR), it is estimated that nine million miss out on the extra support available if they were on the register, such as braille bills for customers with poor eyesight; or getting a meter moved so it's easier to reach for customers with mobility issues.

To encourage disclosure and to make sure that more households receive the help they are entitled to, Citizens Advice plans to create a universal and accessible **online registration process** for the PSR. The first stage in the process was to build a simple tool that points people to the right application form, depending on their energy network and supplier.[17]

The longer-term aim of the project is to have one registration form on the Citizens Advice website for both the energy and water sectors. Two key factors should help ensure that eligible households engage with the new streamlined registration process: firstly, Citizens Advice already has a high volume of traffic to the energy pages of its website (around one million in 2016, according to the expert interviews); and second it is a trusted and well-recognised brand.

The Digital Economy Act 2017

Part five of the Digital Economy Act 2017 gives government powers to share personal information across organisational boundaries to improve public services. Among other things, it allows data-sharing between specified public authorities (such as government departments, Welsh Government, county councils) and energy and water suppliers for the purpose of alleviating fuel and water poverty or improving the health and wellbeing of people who experience fuel or water poverty.[18] DWP could share administrative data that it already holds, for example, with energy and water suppliers to make sure that eligible households receive measures to reduce their energy and water & sewerage bills. This has the potential to make it quicker and easier for eligible households to get help.

There already exists similar data matching arrangements for the Warm Home Discount, focused on older people with low incomes (identified through administrative data). Based on figures published in 2016, more than one million low income pensioners receive an automatic energy bill discount each winter, without the need to fill out an application and with very low operational overheads for suppliers.[19]

What's happening in other sectors: The gambling industry

People who think they spend too much time or money gambling online or in gambling premises can now ask to be self-excluded. This means they ask a company to stop them gambling with that company for at least six months,[20] although there are concerns about how well this works in practice.[21]

It is also possible for people to self-exclude from *all* Licensed Betting Offices that they use or are likely to use, under the Multi-Operator Self-Exclusion Scheme (MOSES). Since its launch in November 2015, it is reported that around 3,500 individuals have registered with the MOSES exclusion scheme and, on average, customers exclude from 22 shops each. In terms of the registration process (the relevant part for our purposes), an early evaluation of the scheme found this was

Building block I – data disclosure

straightforward for most users, but could be improved by supporting customers to register quickly and more conveniently e.g. through online services.[22] A similar multi-operator scheme is expected to be launched for online gambling companies.

Building block 2 – data capture

Financial services firms have well-established systems and processes for capturing customers' financial transaction data and sharing it (for example with credit reference agencies) that are highly structured and closely controlled. Capturing data about someone's (non-financial) vulnerable situation is a very different prospect and one that provoked a lot of discussion in our expert interviews.

As we saw in Part One, there is already some use of vulnerability flags in financial services to capture basic information about an individual's situation. If more, or different, data were to be routinely captured about customer vulnerability, this gives rise to some fundamental questions that have practical implications for data-sharing. Among the questions highlighted in our expert interviews were:

- How should vulnerability be defined from an operational perspective?
- How much information do firms require about vulnerability to make data-sharing worthwhile?
- Is there value in a standard classification of vulnerability?
- Do organisations have the necessary infrastructure for more data capture and greater data-sharing?

We explore each of these questions in turn, drawing largely on our expert interview data.

How should vulnerability be defined from an operational perspective?

For our expert interviewees, defining vulnerability from an operational perspective was seen as a vital first step towards greater data-sharing, but one that is challenging for a number of reasons:

- Vulnerability can apply to many different situations or circumstances, including (but not limited to) physical health, mental health, bereavement, substance addiction, age, physical or psychological abuse.
- It can be complex and multi-faceted.
- It may be an episodic or transitory state.
- It generally involves some degree of subjective judgement.
- What may make one customer vulnerable to detriment may not affect another similar customer in the same way.

An FCA Occasional Paper[23] published in 2015 provides a broad definition of consumer vulnerability that has become widely accepted (Box 2).

Box 2 – Defining consumer vulnerability

"A vulnerable consumer is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care."
(Coppack et al. 2015, page 20)

Building block 2 – data capture

On the one hand, this definition is useful because it is wide-ranging and inclusive. On the other hand, broad definitions will be interpreted in different ways by different organisations in their policies and procedures, depending on factors such as the organisation's business risk appetite, which may change over time.

> *"… it's a bit of a blanket term for a lot of different causes."*
>
> *"… we are all just making it up based on the risk appetite that our own individual businesses have."* (Expert interviews, financial services)

This means that a customer in a vulnerable situation may be treated differently by different firms, or be treated differently by the same firm over time. To move towards greater data-sharing between organisations, for the benefit of consumers, some standardisation or categorisation of vulnerability might be necessary, as we discuss below. Such a classification is no guarantee of standard treatment by organisations, however.

While the forgoing discussion focuses on how organisations define vulnerability, there is the related question of how customers perceive their situation, and how they might wish it described and recorded. Certainly, customers may not see themselves as 'vulnerable' and baulk at the term. We return to this topic later on, in Data Control.

How much information do firms require about vulnerability to make data-sharing worthwhile?

Under GDPR, the collection of personal data should be "limited to what is necessary", rather than "not excessive" (as in the Data Protection Act). As we've already seen in Part One, where used, vulnerability flags currently tend to be high-level (e.g. vulnerable/not vulnerable), sometimes with the potential option of adding explanatory notes. In a different approach, the Vulnerability Registration Service enables individuals to self-exclude from credit and financial promotions that are offered by firms that sign-up to use the service.[24] In other words, the self-exclusion flag relates to a specific response that should be standard across participating firms.

For our financial services expert interviewees, there was a question mark about the value of simple flags or basic information, especially where firms plan to use the captured data to decide their own intervention or 'treatment' strategy.

> *"It's that more granular piece of information to allow us to know what do we need to do for that customer to assist them and how long do we need to do it for?"* (Expert interview, financial services)

They feared that any benefits to consumers of not having to repeatedly give the same information about their situation to different organisations would be lost if organisations required more details from customers in order to offer the right sort of help or support.

Building block 2 – data capture

Is there value in a standard classification of vulnerability?

If sharing simple flags can't provide sufficient information to help organisations respond to vulnerable customers, is there value in a more sophisticated classification of vulnerability that organisations commit to use for data-sharing purposes?

This idea had some appeal among our expert interviewees, provided the classification was comprehensive enough to cover a wide number of vulnerable situations.

> *"… firms could say okay there's 10 categories, we think eight are vulnerable in our world, all 10 may be vulnerable in someone else's world and as that data comes through you say right is it in one of the eight that we'd view as vulnerable, yes, okay right we need to do something with that information"* (Expert interview, financial services)

Various different ways of classifying vulnerable situations were suggested, some of which involve sensitive personal data and other that do not:

- The type of vulnerability e.g. mental health, physical health, terminal illness, life events, low literacy/basic skills.
- The customer's current situation e.g. in crisis, in recovery.
- How the customer is affected and what that means for dealing with organisations e.g. 'finds speaking on the phone difficult, prefers email or webchat'.
- The adjustment that is indicated by a vulnerable situation e.g. 'contact by email or webchat'.

For our expert interviewees, again the key question was whether - when shared between organisations - a standard classification would give them enough information without further contact with customers. Given that different firms have their own policies and procedures for treating customers fairly, this seems doubtful – at least for a wide spectrum of complex vulnerable situations. A standard classification for particular types of vulnerable situation (such as long-term or permanent health conditions) with a fairly standard set of responses or 'treatments' might be more feasible.

Looked at another way, a standard classification might at least allow organisations to short-list a set of possible responses and help open up a conversation with customers. So rather than customers having to repeat all of the same information to more than one organisation, data-sharing using a standard classification could assist a more outcome-focused dialogue.

As the process of developing and agreeing any standard classification of vulnerability would require considerable work (and potential cost for organisations, as we discuss next), its value would have to be carefully weighed against the likely benefits for individuals and organisations. Organisations would have to feel that any investment in a classification system was worthwhile and be confident that the classification met (and continued to meet) their particular requirements.

Building block 2 – data capture

Do organisations have the necessary infrastructure for more data capture and greater data-sharing?

As well as definitional and ethical questions, there is also a very practical question: is more data capture and greater data-sharing possible without having to make significant infrastructure changes?

From our expert interviews, it certainly appeared that many organisations across financial services (and the advice sector) would struggle to capture and share more data about vulnerability within their existing systems. Even capturing and sharing customer data effectively *within* organisations can be difficult, for example if there are different systems within one parent company due to mergers and acquisitions. As a result, internal systems do not always talk to each other and internal data may not flow smoothly across a group of companies.

> *"… our legacy systems don't talk to each other… So that infrastructure thing is, I think, very much on people's minds, you know, have we got the right systems and can we amend them."* (Expert interview, financial services)

The prospect of large-scale infrastructure renewal for the sole purpose of capturing and sharing vulnerability data seems unlikely – and carries its own risks if it requires large-scale data migration from existing to new systems. So any new plans for greater data capture and data-sharing would have to work within current systems constraints, at least in the short term.

What's happening in other sectors: Energy and water

The energy sector has worked through similar issues regarding vulnerability definitions and classifications, so that energy companies can share data in a consistent way in order to better target customers that are eligible for additional non-financial support. The type of non-financial help varies from company to company but includes services such as advanced warning of planned power cuts, priority support in an emergency or meter reading services.[25]

As part of this work, an industry-led group in the energy sector has, over the last two years or so, developed a set of standardised vulnerability Needs Codes (the categories that allow customers to register on the Priority Services Register for non-financial support) that are being rolled out across electricity and gas companies (Figure 5). As Figure 5 shows, these Needs Codes are restricted to certain types of situation where network operators and suppliers may offer services such as priority support in an emergency for medically dependent customers.

Prior to this, there were marked differences in how electricity and gas companies recorded information about customer needs in their registers, which meant that companies could not easily recognise and process incoming data they received from one another.[26] According to our expert interviews, each supplier is responsible for making sure the data on their register is correct, and they may employ Vulnerability Officers or Special Needs Officers to make sure this happens.

Building block 2 – data capture

In an equivalent exercise, the water industry is also working to agree Needs Codes for industry-wide use, aligned to the energy sector where possible so as to facilitate cross-sector data-sharing in the future.

Figure 5 - Standard Needs Codes in the energy sector

Reason for wanting to join

Please select all that apply

Chronic / serious illness

- ☐ Chronic / serious illness

Medically dependent

- ☐ Heart, lung and ventilator
- ☐ Dialysis, feeding pump and automated medication
- ☐ Oxygen concentrator
- ☐ Nebuliser and apnoea monitor
- ☐ MDE electric showering
- ☐ Careline / telecare system
- ☐ Medicine refrigeration
- ☐ Stair lift, hoist, electric bed

Safety

- ☐ Oxygen use
- ☐ Poor sense of smell

Poor mobility

- ☐ Physical impairment
- ☐ Unable to answer door / restricted movement

Age related

- ☐ Pensionable age
- ☐ Families with young children five or under

Communication difficulties

- ☐ Blind
- ☐ Partially sighted
- ☐ Hearing / speech difficulties (inc. deaf)
- ☐ Unable to communicate in English

Mental health

- ☐ Dementia(s)
- ☐ Developmental condition
- ☐ Mental health
- ☐ Additional presence preferred

Temporary

- ☐ Temporary - life changes
- ☐ Temporary - post hospital recovery
- ☐ Temporary - young adult householder

Source: Priestly, 2018 (see footnote 17 for full details)

Building block 3 – data hygiene

Broadly speaking, data hygiene means making sure that data is relatively error-free. For information about vulnerability, which may include sensitive personal data, our expert interviewees focused in particular on the importance of maintaining accurate and up-to-date data in the best interests of customers.

Among other things, the Principles of the GDPR require personal data to be accurate and up-to-date (Box 3). An organisation's Data Controller (the person who determines the purposes and means of processing personal data) is responsible for compliance with the Principles.

Box 3 – GDPR Principles

"Article 5 of the GDPR requires that personal data shall be:

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay…"

For relatively stable long-term circumstances or situations, this may be fairly straightforward. However, as we've already seen, a vulnerable situation might well be episodic or transitory which makes data hygiene more challenging.

> *"… people will tell you things sometimes and you don't hear from them for a long time, and it's actually making sure that that snapshot in time isn't negatively impacting on them."*(Expert interview, financial services)

In these situations, how can organisations maintain accurate data? Our expert interviewees saw two possible ways to do this: an outbound customer contact programme run by the organisation that holds the data; or inbound contact from customers to update their information (or a combination of both).

The Vulnerability Registration Service (a platform for customers to record their personal details) has an outbound customer contact programme. Once a customer has registered, they receive a reminder after three months, which prompts them to update their records if necessary.[27]

Organisations that don't use a centralised service like this could potentially run their own customer contact programmes and share the updated information with other organisations. This risks being costly and duplicative, and inevitably would involve a time lag between the customer disclosing new information and their records being updated. At the same time, if they rely on inbound customer communication, firms' may well end up with out-of-date vulnerability data.

Building block 3 – data hygiene

The same set of issues applies to the removal of data from organisational records. Under the GDPR, there is a right to erasure, which means that an individual has the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing, including when the individual withdraws consent.

What's happening in other sectors: Energy

In the energy sector, the Needs Codes that allow customers to register on the Priority Services Register for non-financial support include temporary reasons for registration: life changes; post-hospital recovery; young adult householder. According to our expert interviews, energy companies are expected to update and clean their register data periodically. For temporary registration reasons, this might involve contacting the customer to check their situation; expiring the data according to a pre-agreed time period e.g. three months; or leaving the code in place until the customer contacts their supplier in the normal course of business, at which point the customer's situation could be discussed and updated.

Building block 4 – data-sharing

Most private and third sector organisations already have a general ability to share information provided this does not breach data protection or any other law. In addition, they should have regard to industry-specific regulation or guidance about handling individuals' information as this may affect their ability to share information. They must also be aware of legal issues that can arise when sharing personal data with public sector bodies.[28]

We look in detail here at three possible models for organisations to share more data about customers in vulnerable situations:

- Company-to-company sharing
- Customer-facing vulnerability register
- Third-party inter-company database

Any data-sharing model can only be as good as the information that is recorded, as we discussed under 'Data Capture'. There is unlikely to be much cost-saving for the organisation, or time-saving for the customer, if organisations have to discuss the situation with the customer again in order to understand the possible options or responses. To work optimally and in the customers' interests, these models also assume similar levels of good practice regarding data collection, use, storage and sharing across all participating organisations. Both these factors are important to build user trust in the data-sharing system.

Unsurprisingly, data security was uppermost in the minds of our expert interviewees when it came to the potential to share more data about vulnerability – and also another crucial factor in building consumer trust. For greater data-sharing to happen in financial services, firms would want reassurances on data security matters such as those set out in Box 4, regardless of the exact model of data-sharing.

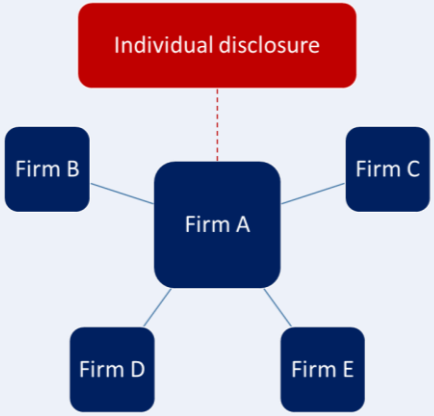
Box 4 – Some of the data security questions that require answers

- How do participating organisations demonstrate that they meet security standards?
- What checks and balances should be in place for data-sharing to happen securely?
- Once my organisation shares data, who is liable for how other organisations use that data?

Building block 4 – data-sharing

Company-to-company sharing

The basic premise of this model is that Company A receives information from a customer about their vulnerable situation and shares this with other firms as agreed with the individual and in line with data protection law.



An example of this data-sharing model is the **Priority Services Register** that operates in the energy industry. Electricity suppliers and electricity Distribution Network Operators (DNOs) are required to establish and maintain a Priority Services Register (PSR) of customers. They record information about vulnerable customers (disclosed by the customer to the supplier) using Needs Codes and hold these against customers' accounts so they can provide appropriate services.

Energy suppliers are required by their licence conditions to share appropriate information with the relevant distribution network; and DNOs must share information about customers they have added to their PSR with electricity suppliers. As we saw earlier, the energy sector has produced a standard set of Needs Codes for use across suppliers and DNOs; and work is ongoing to increase data-sharing between energy companies (and eventually water companies as well) so that customers only have to sign up once for non-financial help.

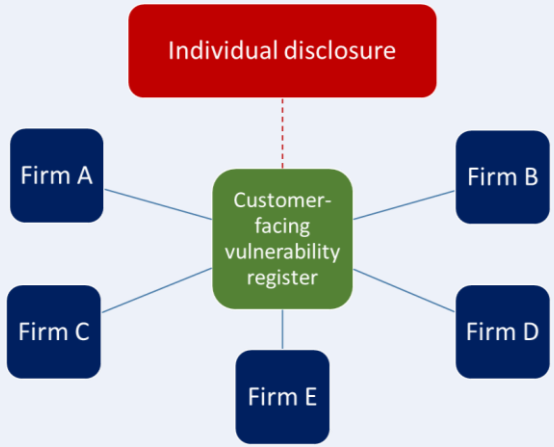
In government, **the Department for Work and Pensions (DWP) Tell Us Once Service** also works on this model**.** Provided their local Register Office offers the service, individuals can use Tell Us Once to report a death[29] or birth[30] to various government organisations in one go. The bereavement service can be accessed online, by telephone or in a face-to-face appointment.[31] After registering a birth, the service is accessed through a face-to-face appointment. The service re-uses established infrastructure, such as existing business processes and information systems, and recognises that staff skills already exist to deliver the service. In a survey in 2012 of those who had used the service, 99.5% of responses were positive.[32]

In financial services, there exist **individual partnerships between creditors and advice agencies** to share data via this company-to-company model. For example, creditors 'hotkey' to external sources of support or arrange for another organisation to call-back the customer.

Building block 4 – data-sharing

Customer-facing vulnerability register

This model is built around a central third-party data repository. The individual adds themselves to the data repository (or a relative with Power of Attorney does this for them). Depending on the systems used, organisations (such as creditors and debt collection companies) either search this database when necessary (e.g. when an individual applies for a new product or falls into arrears) or they are automatically updated of the individual's situation.



In our expert interviews, respondents could certainly see operational advantages to a single repository for vulnerability information that is collected and recorded in a standard way (although a conversation with the customer might still be required).

For this model to function optimally, ideally individuals would proactively disclose their situation to the data repository, and could be prompted to do that, for example by their GP following diagnosis of a serious illness. Preferably, most or all of their creditors would also be signed up to the service, otherwise individuals may be left unclear about which organisations they need to contact about their situation and which they do not. Companies could also upload their own customer data to the data repository, to be shared with other organisations (provided they have consent from the individual).

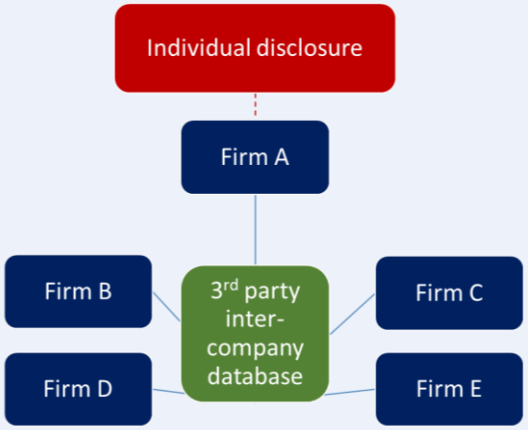
The Vulnerability Registration Service (VRS), launched in March 2017, is an example of a consumer-facing vulnerability register. Individuals (or those with Power of Attorney) sign up to the VRS and therefore define themselves as 'vulnerable'.[33] Once registered, individuals can self-exclude from credit and financial promotions. This information is then shared with firms that have signed up to the service, when they search for an individual in the database.

Another potential use is for energy and water companies to share information via the VRS about registered consumers who require non-financial support services.[34]

Building block 4 – data-sharing

Third-party inter-company database

In a third-party inter-company database model, Company A receives information from a customer about their vulnerable situation and shares this with a third-party database provider, in line with data protection law. Other companies can be notified if one of their customers is added to this database or they can search the database themselves.



An example of this data-sharing model is a **Credit Reference Agency** (CRA). CRAs hold customers' credit records (and various other information), which are stored and processed by the CRA but searched, say, by lenders during customers' credit applications. Crucially, information from lenders about customers' accounts is included on the credit record, indicating that it is possible for such information to be shared with third-parties.

The idea of extending CRA data to include information about vulnerability (e.g. in the form of vulnerability flags) was raised in our expert interviews, and has been discussed more widely in the industry. The potential advantages are that CRAs have the infrastructure for data-sharing; there exists a set of guidelines that govern the sharing of data via CRAs[35]; they already comply with firms' own security standards; there is a process to validate data shared with CRAs; and here is a procedure for individuals to correct their CRA data (the Notice of Correction – which we discuss in more detail below).

For this model to work, it requires some standard system of defining or classifying vulnerable situations, as we discussed in 'Data Capture'; which in turn could well require organisations to make significant changes to the data they share with CRAs. An optimal model (from a consumer perspective) would see data shared with all of the main CRAs.

Notice of Correction

Another option could be to extend the CRA Notice of Correction as a way for individuals to share vulnerability information. Individuals have a legal right in the Consumer Credit Act (1974) to add a Notice of Correction to their credit report if they feel something is misleading or they want to provide an explanation. Any organisation searching the credit report in the future or who has seen it in the previous six months sees the Notice of Correction (NOC), and they must take account of it when the individual applies for credit.[36]

According to our expert interviews, NOCs have come to be used for a range of other information e.g. for people to identify that they are in the Armed Forces (which can mean frequent house moves, something that might impact on their credit rating). This raises the possibility of individuals using NOCs to share vulnerability information. The benefit is the ability to piggy-back on an established system. However, in their

current form NOCs may not provide an optimal way of recording and sharing vulnerability data for data capture and data hygiene reasons:

- There exists a 200 word limit that may not be sufficient for someone to explain their vulnerable situation.
- Individuals have to make an NOC with all the CRAs if they want full coverage.
- Individuals would have to update their NOC if their situation changed, which in turn relies on organisations checking the NOC on a regular basis.
- The information would have to be in a format that allows organisations to know how to respond; and different organisations may use the data differently (which as we've seen is a common risk across any model of data-sharing).

Blockchain: A new way to securely share personal data?

Blockchain technology (see Box 5) could be another way for individuals and organisations to securely share personal data - and allow individuals close control over the ways in which their data are shared and used (a topic we return to later). This relatively new technology opens up the possibility of:

> *"… an environment in which data can easily be shared across systems but in which individuals and organizations can take back ownership of their data and control the flow of personal information—who sees it, what they see, and when."* [37]

For example, at any given time an individual may alter the set of permissions for their data and revoke access to previously collected (or shared) data.[38]

Box 5 – What is blockchain?

A blockchain is an encoded digital ledger that is stored on multiple computers in a public or private network. It can therefore exist without a centralized authority or server managing it.[39] It comprises data records, or "blocks." Once these blocks are collected in a chain, they cannot be changed or deleted by a single actor; instead, they are verified and managed using automation and shared governance protocols.[40] This makes it very difficult for anyone to tamper with information that has already been agreed.[41] Strong encryption (the process of converting information or data into a code) reduces the risk of unauthorised access to data.[42] A decentralized system should also make legal and regulatory decisions about collecting, storing and sharing sensitive data simpler.[43]

In financial services, blockchain is seen as a way to overhaul outdated back office systems, speed processes and reduce costs.[44] It could be used, for example, to provide a record of identity or to store validated 'know your customer' information[45,46] or potentially to store or provide information about someone's vulnerable situation.

Building block 5 – data control

In the preceding discussion, the complex issue of data control has been considered mainly from an operational perspective – for example, how do organisations exercise control over vulnerability data in order to comply with law and regulation, but also to protect their own systems, processes and customers? But what about personal control over data-sharing and data use that individuals could or should exercise?

When it comes to controlling data access and use, there seems to be three schools of thought about achieving a balance between the interests of individuals and those of organisations: regulating data use as well as data collection; more transparency; and personal data management.

These three approaches do not have to be mutually exclusive. We describe them below. In addition, the evidence suggests that individuals need to be engaged on these issues as citizens (deliberating on the conditions and safeguards) as well as consumers (agreeing or disagreeing to terms of service).[47]

Regulating data use

In the first school of thought, legal experts (such as Oxford University's Viktor Mayer-Schönberger) argue that the *use* of data should be regulated as well as its collection. Online firms could be prohibited from using certain data or using them in such a way that could cause harm to an individual. This would shift responsibility towards data collectors and data users who should be held accountable for how they manage and use data, rather than relying on obtaining individual consent, where defining and operationalising informed consent is challenging, particularly given the volumes of data that are available about individuals.[48]

More transparency

The second school of thought centres on encouraging greater transparency when it comes to data collection and use, for example looking at how privacy notices can provide individuals with better information[49] and (in the field of health at least) proposing more 'granular' privacy controls:

> *"Persisting concerns dependent on changes to the context, personal circumstances and preferences, indicate that 'granular' privacy control over which health information should be shared with whom remains an important issue…"* [50] (page 12)

There are moves in the health field and biobanking in particular - where people opt to share health data with the UK Biobank for research purposes – towards a *"technologically-mediated form of dynamic consent"*.[51] This new approach aims to allow individuals to change their consent preferences over time, in recognition that (1) initial consent may not have been fully informed, and (2) the consent process might have been engineered to encourage consent.

Building block 5 – data control

Personal data management

In a 2011 publication, the World Economic Forum noted the emergence of personal data services which:

> *"… provide the safe means by which an end user can store, manage, share and gain benefit from his or her personal data… Personal data services consolidate end users' digital identity, allowing them to control which third parties are entitled to access – along with how, when and at what price."* [52]

As we saw with blockchain, the main advantage of a personal data service is that an individual's identity is validated and assured, reducing the risk of fraud for the end-user and the organisations that they share data with. It can also simplify data management, for example by doing away with the need for multiple passwords.

An example of a personal data service in the UK is Mydex, a Community Interest Company. The Mydex Platform has components for personal data management, consent management and identity management that organisations can use, for example to comply with regulation or incorporate them into their existing processes.[53] Individual users have a Personal Data Store (which is free of charge) and choose what data they want to store and potentially share.[54] Users can create their own set of verified proofs about their situation (e.g. their identity) and store a verified copy of the data on their personal data store which they share and manage themselves (Figure 6). Only the individual can see the data held in their Personal Data Store, and when they share it, it is visible only to them and the third party to whom they have given access. This means there are not multiple copies of data sat in multiple different organisations, therefore reducing the risk of unauthorised access.

Figure 6 – Mydex personal data store (source: Mydex CIC, 2017)

Building block 5 – data control

Mydex is also one of the partners in a project to co-design, test and deliver local, digitally-enabled and person-centred energy advice services to citizens in Renfrewshire, Scotland.[55]

> *"… it's picking up the personal data and moving into an idea of components, open inter-connectable components that you can slot together to solve a problem, instead of 'walled gardens' or silos of personal data held separately, outside of the individual's reach."* (Expert interview, Mydex)

Another example of a personal data service is the US Department of Health & Human Services 'Blue Button' initiative which is part of a wider 'My Data Initiative'.[56] This is a web-based feature that allows patients to easily download all their historical health information from one secure location and share it with healthcare providers, caregivers, and others they trust.

Open Banking

Among our expert interviewees, there was also interest in the opportunities that Open Banking (Box 6) might offer to help people manage their own data – initially financial transaction data, but potentially also vulnerability data. An individual might, for instance, be able to give an aggregator service access to their data, that could then be on-shared with other organisations as determined by the customer, for example via a data dashboard where they could switch access to their data on or off.

Box 6 - What is Open Banking?

The launch of Open Banking in the UK in January 2018 is the result of regulatory intervention to encourage innovation and improve competition in the current account market. Open Banking describes "*a secure set of technologies and standards that allow customers to give companies other than their bank or building society permission to securely access their accounts.*"[57]

Ultimately, the aim of Open Banking is to make it easier for consumers to manage all their accounts and bills through a single digital platform, with the option of allowing apps and price comparison websites to use consumers' own financial data to offer personalised and intuitive services and as a result stimulate innovation and competition.[58, 59]

Steps towards greater data-sharing between organisations

Can greater sharing of data between financial firms bring benefits to firms and consumers alike – especially where customers in vulnerable situations are concerned?

We carried out this research to shed light on data-sharing between financial services organisations, an area that has received relatively little attention to date. While our focus was on sharing data about vulnerability, many of the lessons from the research could apply to data-sharing generally. By opening up this complex area to scrutiny, the study surfaces the key issues and challenges that firms and regulators need to consider in terms of data-sharing between organisations, including options for giving individuals control over the type and amount of data that is shared.

Our evidence shows some considerable potential benefits for individuals and organisations of greater data-sharing, provided the risks are properly monitored and managed. From our expert interviews, it was clear that financial services firms are interested to explore greater data-sharing between organisations, and interested in learning from the experience of other sectors.

This interest was tempered with nervousness about handling a wide spectrum of potentially sensitive personal data. To help organisations work-through the thorny questions about how data-sharing might work in practice we considered five building blocks for greater data-sharing – data disclosure; data capture; data-sharing; data hygiene; and data control – and looked to learn from other sectors' experiences of working to share data in the interests of individuals.

So what might the next steps be towards greater data-sharing among financial services organisations? While challenging, our expert interviewees did not want to relegate vulnerability data-sharing to the 'too difficult pile'.

> *"I think it would be wrong of us to say this is all too difficult… there may well be elements that could be the pilots or the early stages of us sharing data more efficiently."* (Expert interview, financial services)

Three possible next steps might be:

- For firms to look at ways to achieve better data-sharing within their own organisation or corporate groups.
- To undertake proof of concept work; for example, pilots to share data for one type of vulnerability, such as one or more long-term health conditions or disabilities.
- To explore the feasibility of a shared way of classifying vulnerability.

If individuals or organisations want to take these (or other) steps forward, we believe our research findings offer a useful starting point.

If you work for an organisation that is considering how to make better use of your data to support customers in vulnerable situations, we would love to hear from you! Please get in touch with Professor Sharon Collard at sharon.collard@bristol.ac.uk

Appendix

Organisations that took part in our Expert Interviews

Citizens Advice (energy and debt teams)

Consumer Council for Water

Consumer Finance Association

Equifax

Experian

Finance and Leasing Association

Flexys

Lending Standards Board

Money and Mental Health Policy Institute

Mydex

Southern Water

StepChange Debt Charity

Vulnerability Registration Service

We conducted a small number of interviews with other organisations that wished to remain anonymous.

Endnotes

[1] Fitch, C., Evans, J., & Trend, C. (2017). *Vulnerability: a guide for debt collection. 21 questions, 21 steps.* Bristol: Personal Finance Research Centre. Available at http://www.bris.ac.uk/media-library/sites/geography/pfrc/pfrc1701-21-steps-vulnerability-and-debt-collection-(web).pdf

[2] MALG (2015). *Good practice awareness guidelines for helping consumers with mental health conditions and debt.* Third Edition. Available at http://www.moneyadvicetrust.org/SiteCollectionDocuments/Research%20and%20reports/MALG_web%20based%20version%2023.3.15.pdf The first edition was published in 2007, the second in 2009.

[3] FCA (2016). *Our Future Mission*. London: Financial Conduct Authority. Available at: https://www.fca.org.uk/publication/corporate/our-future-mission.pdf

[4] *Data Protection Act 1998*. Norwich: Stationery Office Available at http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

[5] For more information, visit the GDPR Portal http://www.eugdpr.org/

[6] Fitch, C., Evans, J., & Trend, C. (2017). *Vulnerability: a guide for debt collection. 21 questions, 21 steps.* Bristol: Personal Finance Research Centre.

[7] Data from Fitch, Evans & Trend (2017). Note that staff dealt with an average of over 600 customers and third parties in a typical calendar month.

[8] To keep the survey reasonably short, we did not ask why respondents had disclosed this information. Government departments such as DWP may require people to disclose this sort of information in order to access financial or non-financial support.

[9] Mind (2011). *Still in the red. Update on debt and mental health.* London: Mind. Available at: https://www.mind.org.uk/media/273468/still-in-the-red.pdf

[10] Anyone with experience of mental health problems was invited to take part in the 2011 Mind survey. Our 2017 online survey respondents also have experience of mental health problems but have opted in to MMHPI's Research Panel because of their interest in financial issues.

[11] Money and Mental Health Policy Institute (no date). *Travel insurance and mental health: a turbulent journey*. Available at https://www.moneyandmentalhealth.org/travel-insurance-mental-health/

[12] For example: Financial Conduct Authority (2018). *Consumer Credit Sourcebook (CONC)* – CONC 7.2 Clear effective and appropriate arrears policies and procedures. Available at https://www.handbook.fca.org.uk/handbook/CONC/7/2.html

[13] See for example: Which? (2017). *Select Committee Evidence. Public Accounts Committee: The Growing Threat of Online Fraud*. Available at https://www.parliament.uk/documents/commons-committees/public-accounts/Correspondence/2017-19/evidence-which-online-fraud.pdf.

[14] European Commission (2015). *Special Eurobarometer 423 – Cyber security.* Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

[15] UKRN (2017). *Making better use of data: Identifying customers in vulnerable situations. A report for water and energy companies.* Available at http://www.ukrn.org.uk/wp-content/uploads/2017/10/Making-better-use-of-data-identifying-customers-in-vulnerable-situations.pdf

[16] The UKRN is a network formed by 12 of the UK's sectoral regulators. It was established by its members in 2014, to provide the structure for regulators to consider common issues and policy projects with relevance across utility, financial and transport sectors. For a list of members and more information, visit http://www.ukrn.org.uk/about-ukrn/

[17] Priestly, O. (2018). *9 million people are missing out on support with their energy supply.* Available at https://wearecitizensadvice.org.uk/9-million-people-are-missing-out-on-support-with-their-energy-supply-fb3744474b6e

Endnotes

[18] *Digital Economy Act 2017 Chapter 30*. Norwich: The Stationery Office. Available at https://www.legislation.gov.uk/ukpga/2017/30/pdfs/ukpga_20170030_en.pdf

[19] DECC (2016). *Warm Home Discount Scheme.* London: Department of Energy & Climate Change. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/514324/Final_Warm_Home_Discount_consultation_for_publication.pdf

[20] Gambling Commission (no date). *Tools you can use to help you control the time and money you spend gambling*. Available at http://www.gamblingcommission.gov.uk/for-the-public/Safer-gambling/Tools-to-help-you-control-your-gambling.aspx

[21] BBC.CO.UK (2017). *Self-exclusion scheme in betting shops flawed.* Available at http://www.bbc.co.uk/news/av/uk-42372860/self-exclusion-scheme-in-betting-shops-flawed

[22] Chrysalis Research (2017). *Evaluation of the Multi-Operator Self-Exclusion Scheme (MOSES). A report for MOSES.* Available at https://about.gambleaware.org/media/1467/jn175-moses-evaluation-report-final-report-230317.pdf

[23] Coppack, M., Raza, Y., Sarkar, S., & Scribbins, K. (2015). *Consumer vulnerability. Occasional Paper 8*. London: Financial Conduct Authority.

[24] UKRN (2017). *Making better use of data: Identifying customers in vulnerable situations. A report for water and energy companies.* Page 24.

[25] Ofgem (2018). *Priority Services Register for people in need*. Available at https://www.ofgem.gov.uk/consumers/household-gas-and-electricity-guide/extra-help-energy-services/priority-services-register-people-need

[26] UKRN (2017). *Making better use of data: Identifying customers in vulnerable situations. A report for water and energy companies.*

[27] Ibid. Page 24.

[28] Information Commissioner's Office (2011). *Data-sharing code of practice*. Page 12.

[29] GOV.UK (no date).*What to do after someone dies.* Available at https://www.gov.uk/after-a-death/organisations-you-need-to-contact-and-tell-us-once

[30] GOV.UK (no date). *Register a birth.* Available at https://www.gov.uk/register-birth

[31] Bereavement Advice Centre (2017). *The tell us once service.* Available at https://bereavementadvice.org/topics/registering-a-death-and-informing-others/tell-us-once-service

[32] HM Government (2012). *Overview of Tell Us Once. Presentation given on 8th November 2012*. Available at https://www.kingsfund.org.uk/sites/default/files/steve-scott-tell-us-once-programme-a-nationwide-programme-to-improve-citizen-experience-nov12.pdf.pdf

[33] https://www.vulnerabilityregistrationservice.co.uk/

[34] UKRN (2017). *Making better use of data: Identifying customers in vulnerable situations. A report for water and energy companies.* Page 24

35 SCOR (the Steering Committee on Reciprocity) is a cross industry forum made up of representatives from credit industry trade associations, credit industry bodies and credit reference agencies. It is responsible for the administration and development of the data-sharing rules known as the Principles of Reciprocity. The Principles of Reciprocity are a set of guidelines governing the sharing of personal credit performance and related data via the closed user groups of UK credit reference agencies. For more information visit http://www.scoronline.co.uk/

[36] Where there is a Notice of Correction, lenders must manually check these credit applications rather than a computer making the decision. This means that customers may need to provide extra information or answer more questions, so the application takes longer as a result.

[37] Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017). *Using blockchain to improve data management in the public sector.* McKinsey & Company. Available at https://www.mckinsey.com/business-functions/digital-

Endnotes

mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector

[38] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Security and Privacy Workshops 2015 IEEE.* Available at http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=7163223

[39] Ray, S. (2018). *The difference between blockchains and distributed ledger technology.* Available at https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92

[40] Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017). *Using blockchain to improve data management in the public sector.* McKinsey & Company

[41] Ali, R., Barrdear, J., Clewes, R., & Southgate, J. (2014*). Innovations in payment technologies and the emergence of digital currencies*. Available at https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/quarterly-bulletin-2014-q3.pdf?la=en&hash=874BAD99E54170C8DB5C082D6E8962D3F10997DF

[42] Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017). *Using blockchain to improve data management in the public sector.* McKinsey & Company

[43] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Security and Privacy Workshops 2015 IEEE.*

[44] Collard, S.,Coppack, M., Lowe, J., & Sarkar, S. (2016). *Access to financial services. Occasional Paper 17*. London: Financial Services Authority. Available at https://www.fca.org.uk/publication/occasional-papers/occasional-paper-17.pdf

[45] VALID (2017). *Procivis launches blockchain-based personal data management platform VALID, building on the successful rollout of its eID+ digital identity solution*. Available at https://blog.valid.global/procivis-launches-blockchain-based-personal-data-management-platform-valid-building-on-the-5018180a7b04

[46] Wild, J., Arnold, M., & Stafford, P. (2015). *Technology: Banks seek the key to blockchain*. Available at http://www.ft.com/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html

[47] Sciencewise (April 2014). *Big Data. Public views on the collection, sharing and use of personal data by government and companies*. Available at http://webarchive.nationalarchives.gov.uk/20170110135457/http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf

[48] The Economist (2017). *Fuel of the future. Information is giving rise to a new economy. How is it shaping up?* 6 May 20-17, pages 17-20.

[49] ICO (2015). *Data protection rights: What the public want and what the public want from Data Protection Authorities*. Available at https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf

[50]Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC Medical Informatics and Decision Making* 15:86

[51] Whitley, E. A. (2013). Towards effective, consent based control of personal data. *Digital Enlightenment Yearbook 2013.* Editors: Hildebrandt, M., O'Hara, K., & Waidner. M. Netherlands: IOS Press.

[52] World Economic Forum (2011). *Personal data: the emergence of a new asset class*. Available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[53] Mydex CIC (2017). *Unlocking the power of our data.* Available at https://medium.com/mydex/mydex-cic-white-paper-unlocking-the-value-of-our-data-the-individual-as-the-point-of-integration-cb5cc1f9f9f3

[54] https://mydex.org/about-mydex

[55] Alexander, D. E. (2018). *Overview of EPCAS Project.* Available at https://medium.com/epcas/overview-of-epcas-project-843d20bee105

[56] Other projects are the Green Button (for personal energy usage data) and the Red Button (for personal educational data) https://en.wikipedia.org/wiki/Blue_Button

Endnotes

[57] Open Banking Implementation Entity (2017). *UK's Open Banking to Launch on 13 January 2018.* Online press release, 19 December 2017. Available at https://www.openbanking.org.uk/about-us/news/uks-open-banking-launch-13-january-2018/

[58] Edmonds, T. (2018). *Open Banking: Banking but not as we know it?* London: House of Commons. House of Commons Library Briefing Paper Number 08215, 26 January 2018.

[59] Cavaglieri, C. (2018). *Open Banking: Sharing your financial data*. Available at https://www.which.co.uk/money/banking/switching-your-bank/guides/open-banking-sharing-your-financial-data