'Midata' consultation

Open Rights Group response.
September 2012

More detail about this consultation can be found on the Department for Business, Innovation and Skills' website[1]. For more information about this response or Open Rights Group's work on this issue contact Peter Bradwell, peter@openrightsgroup.org

Question 1: Do you agree with the principles of midata? Have you any comments on the proposed approach?

- Yes. Personal data generated by individuals belongs to the individual. It should be easy for the individual to obtain in standard reusable formats.

- Midata should also help people start to understand the scale of data collection and use about them, and the extent to which personal data is used / abused without their knowledge or consent.

- That is not to say it is without risk. These risks need to be brought into the light and addressed, not glossed over and ignored.

- Making the individual the central point in decisions about the use of their personal information will require a strong legal and procedural framework. This is the only way to ensure that the proposals work to the benefit of individuals, including legal and procedural safeguards and information and educational resources.

- ORG supports the empowerment of the individual online. People having control over their personal information furthers this aim when it gives them more of a say about when and how information about them is disclosed and used, and more of a hand in deciding what it says about and does for them.

- However, this can only happen where the is the right 'support system', including a more robust framework of personal data rights, services to help manage the data and educational resources. People need to trust those they are dealing with, not be exploited, with no unreasonable Ts&Cs, strong principles of data minimisation, stronger implementation and execution of the DPA, and clear rights to revocation and deletion.

- Midata is not just about switching suppliers. It cannot be seen in isolation from the wider agenda about the control and value of personal data. It's linked with data protection, ID assurance and integrated lifestyle management as well as with marketing, choice and competition.

- So whilst supporting the development of the midata programme, progress of this agenda needs to go hand in hand with the strengthening of related privacy rights. For example, the UK Government should support the proposed EU draft Data Protection Regulation in its current form (which builds in strong rights to delete and to obtain data). These are minimum necessary safeguards. We suggest it is incoherent and dangerous for the government to simultaneously enable a data market based on personal information and oppose the new data protection regime proposed in Europe.

1 http://www.bis.gov.uk/Consultations/midata-review-and-consultation?cat=open

- Support for accredited, trusted data services should complement this robust data protection regime.

Question 2: Do you have a view on whether particular sectors or types of business should or should not be covered?

- It is also helpful to consider a map of who the players are in the wider ecosystem of which midata is a part. There are at least three kinds of entities in this:
    - Individual: formerly known as the data subject
    - Personal data service: offering to store personal data securely and and help people manage third parties' access to it without themselves having access to it.
    - Businesses who exploit data as part of / to offer services (of which there are many types)

- It should be clear from the start that midata should include information from public services such as health, education and jobseeking.

- There will be exceptional cases where effective services or confidentiality (eg psychiatric services, child protection) are compromised by the service provider sharing data with the client.

Question 3: What is your view on the likely impact of the proposed approach on privacy, consent and information security and the implication for data protection?

- The organisation returning the data needs to knows precisely to whom it is going and that they are authorised to receive it. This requires authentication and ID assurance.

- The individual needs to be properly equipped to receive and store personal data safely.

- The midata programme be much more closely aligned with the discussions about ID assurance and the MoJ's work on the draft Data Protection Regulation. It makes no sense for BIS to pursue Midata only for the MoJ to undermine this by pushing back against the draft Data Protection Regulation on the ground that they impose undue burdens on business.

- For example, midata can be seen as an extension of the Data Protection Act subject access request.

- The problems with companies making broad and inappropriate usages could be combated by effective enforcement of strong data protection rights, such as the right to delete. In the absence of these rights, UK consumers could be vulnerable to the abuse of their data with their apparent consent.

- To ensure data works to the benefit of individuals a robust set of safeguards and resources will be necessary. Not all of these are within the remit of the midata programme. So they will require some joined up thinking and policy making. For example:
    - Midata must be accompanied by robust rights to delete data and to revoke consent, with stronger enforcement of DPA Principle 3 around data minimisation. That requires, for example, the UK Government and in particular the MoJ

- The legal agreements and contractual terms on which personal data are shared must protect the individual - restricting subsequent reuse in a way that is clear and acceptable to the individual.
- There will need to be robust ID assurance.
- There will need to be strong sanctions for those who abuse midata so individuals whose data is misused have clear and easy routes for redress.
- There will need to be educational resources on what is at stake: "here's what goes on today"; "how to keep your personal data safe".

- ORG also expects a competitive and healthy choice of personal data services that meet high standards of security, interoperability and usability.

- People need to be confident of who they are sharing their information with. So ID assurance must work both ways - people should be able to verify that organisations they are sharing with are legitimate and meet high standards. They must be strongly regulated and audited.

- Individuals will be free to make their own arrangements. There is a broader security issue with users taking back their data and storing it themselves. This can't outweigh their right to have it back but it does deserve consideration.

Question 4: What is your view on who should have the right to request data?

- Clearly an individual who is suitably authenticated (eg logged into a bank or energy account system) should be able to request data.

- It is desirable that someone with power of attorney can also do this.

- The question of parental requests for children's data is more complex than generally acknowledged/recognised. Children might rightly assert control over some types of data from an early age (gaming, social networks, preferences) while the ages of consent for other data (education, health) is likely to be specific in each case but not all the same. There is no one single easy answer.

- We do not believe that further automated access by third parties (extension of the credit agency model) is in the individual's interests. There is a clear risk in a world where Midata is the norm that service providers say "I'll give you the service but only if you give me widespread access to your personal data, since that is now possible". Only the data necessary for the transaction in hand should be required; the passing of any other data should be a matter for fair equitable trading and informed consent. A person may wish to sell their health records, but it is not tolerable to say you cannot have access to a basic essential service without handing over excessive private data.

- In reality the current default 'Web 2.0" position is that if people want to search the Internet or use smart phones they do indeed hand over far more personal data than is essential or healthy. This is an existing problem to address; it's essential that Midata should protect against further exacerbating it.

Question 5: Some consumers already shop around, though may not always switch to the best deal for them. What additional proportion of consumers is likely to become empowered by this data?

- All consumers will be empowered by having more relevant data at their disposal, but we do not necessarily know just how. It may be in unforeseeable ways. It is far from self-evident that the main purpose to which people will put midata will be to use it to change suppliers.

Question 6: What types of new services might be offered by intermediaries (such as, price comparison websites) and what could be the value of this new market?

- The point of midata is it means the individual can be the point of integration, instead of assorted organisations trying to provide complete services with partially complete, semi-accurate data they have gathered about the individual. This will go beyond price comparison and will encompass any service that can be built on 'permissioned' flows of data, such as services that help people manage their finances, health and energy supply.

Question 7: Should a consumer be able to require the business to supply the data in electronic format directly to a specified third party?

- No. There is a real risk this will be open to abuse. For example, an unscrupulous organisation may offer small sums for access to a person's broad set of 'midata', with broad terms and conditions for reuse. This would effectively simply multiply current problems of inappropriate data retention and sharing.
- It may be safer to require that the data is clearly and auditably released to a place which is clearly (contractually and technically) controlled by the individual, before a separate auditable process sees the individual release it from their own clear and unambiguous control to a third party.

Question 8: Should a third party who is duly authorised by the consumer be able to seek the consumer's data in electronic format directly from the supplier?

- See above. There may be some exceptions, for example in medical emergencies ("in the event of xyz then have immediate access to this sensitive data, but be aware you will leave an audit trail"). Other exceptional cases could include power of attorney and joint accounts.

Question 9: What, if any, requirements should be placed on the secondary users of such data, albeit under the direction of consumers e.g. switching and advice sites?

- The data needs to be passed to the individual without any preconditions, no "intellectual property" controls or restrictions. EDF or Lloyds TSB may not like it if a customer uses their Midata to show their tariffs are too high, or their customer call centre is unresponsive, but they cannot control that.
- As noted above, the legal agreements and contractual terms on which 'midata' personal data are shared must protect the individual - restricting subsequent reuse to those specified clearly upfront, for example.

Question 10: The Government is minded to require businesses to give their customers access to transaction and consumption data, in order to help them better understand their behaviour.
a) What types of data would be most helpful? b) Over what period should the data refer to?

- You can't predict this or legislate for it. The experience of open data is you do not know to what creative uses data sets will be put.

- You might more usefully ask where is it easiest to start, and the answer might be with data already available in portals, electronic bills or online statements. But the destination is that individuals can easily retrieve from public and private sector organisations any structured data about themselves, including recordings of phone calls, proposals, location data, guarantees and receipts, credit scoring and marketing, behavioural analysis.

Question 11: Should other types of information, such as warranties or terms and conditions, be included?

- Yes - see above. And this list is not exhaustive. The more useful question is whether there any data about the individual that specifically should be excluded, and what are the substantive reasons why this is the case.

Question 12: Should the Government specify a particular electronic format beyond a machine readable open standard format in which the data has to be supplied?

- The format is important, but experience suggests that legislation or government specification is not the right way to do it. Perhaps organisations such as W3C or the new ODI have a role here.

Question 13: Should data be made available immediately (e.g. at the click of a button) or should the Government specify a period within which data must be released electronically following a consumer's request? If the latter what would be a reasonable period within which data must be released?

- It should be at the click of a button. It should be as easy as downloading data from a web site, for the very good reason that in all probability that is exactly what it will be.

Question 15: Should businesses be permitted to charge a consumer for providing them with the data in electronic format?

- No. And ORG would not charge its members for returning their data.

Question 16: Should any such charges be constrained by the legislation? If so, do you have a view on how a maximum charge should be set or adjusted?

- See above. There should be no charge.

Question 17: Which body/bodies is/are best placed to perform the enforcement role for this right?

- The small claims courts.

Question 18: Should the Government specify a lead enforcement body?

- No, The ICO has a vital role but is overburdened, underresourced and insufficiently effective already.

Question 19: How should the right be enforced by any such body? Will they need any new powers to enable them to enforce it?

- If the standard fine for consistently failing to produce midata were £4995 then individuals could pursue them through the small claims courts which are quick and effective.
- The Government should also consider highlighting organisations which conform to best practice and regulatory standards.

Question 20: What examples of existing regulatory actions could be reduced or removed if the power being consulted on was exercised?

- It really addresses problems of data protection: holding more data than is necessary, holding inaccurate data, and using data for purposes other than for which it was gathered. Midata will shine a light on these practices by showing individuals what data organisations hold on them. In this sense it is like a free, faster and more effective subject access request.
- The data and its use could be of interest to the OFT where discriminatory pricing or business practices are demonstrated.
- Midata could become a powerful means of providing auditable proof of claims. It may help prove entitlements which are dependent on status held by an organisation: disabled person's entitlement to the lowest energy tariff, or anything that depends on a credit rating or proof of address.

Question 21: Should a consumer be able to launch independent action (and, if so, what sort of action) in relation to non-compliance with the duty?

- See above. Small claim seems easiest.

Question 22: Do you foresee any risks or undesirable consequences from exercising a power to require certain data to be released electronically?

Yes, there are several.

- When people realise how much data is held on them, without their ever feeling they consented to it, they will be startled and dismayed, perhaps angry also.

- There is a danger that if people hold more of their personal data in easily releasable structured formats they will be asked for far more data. This may happen under the pretext of security or risk management (eg fraud prevention). It may be used for profiling and marketing. ORG believes a stronger regulatory solution may be necessary to prevent businesses requiring more personal information than is demonstrably necessary for the purpose in hand.

- People are not yet equipped to manage this much personal data. This needs tools, rules and education.