moz://a

November 19th, 2021
Domestic Data Protection team
DCMS
100 Parliament Street
London
SW1A 2BQ
Via email to: DataReformConsultation@dcms.gov.uk

Re: Response to the Open Consultation on Data: A New Direction

To the Domestic Data Protection team,

Thank you for the opportunity to comment on the Department for Digital, Culture, Media and Sport ("DCMS") open consultation on the UK's data protection regime titled "Data: A New Direction".[1]

Mozilla is the maker of the open-source Firefox web browser, the Pocket "read-it-later" application and other products and services that collectively are used by hundreds of millions of individuals around the world. Mozilla is also a global community of contributors and developers who work together to keep the internet open and accessible for all. As a mission-driven technology company and a non-profit foundation, we are dedicated to putting people in control of their online experience, and creating an internet that is open and accessible to all. To fulfill this mission, we are constantly investing in the security of our products, the privacy of our users and in advancing the movement to build a healthier internet.

General Comments

For Mozilla, privacy is not optional. It is an integral aspect of our Manifesto, which states that individuals' security and privacy on the internet are fundamental and must not be treated as optional. We actualise this belief by putting privacy first in our own products with features like Enhanced Tracking Protection (ETP)[2], Total Cookie Protection (TCP)[3], DNS over HTTPS[4] and our end to end encrypted Firefox Sync service.[5] We also promote privacy in our

[1] Data: a new direction, https://www.gov.uk/government/consultations/data-a-new-direction
[2] Latest Firefox rolls out Enhanced Tracking Protection 2.0, https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/
[3] Firefox 86 Introduces Total Cookie Protection, https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/
[4] Firefox continues push to bring DNS over HTTPS by default for US users, https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[5] Privacy by Design: How we build Firefox Sync, https://hacks.mozilla.org/2018/11/firefox-sync-privacy/

public advocacy, having engaged with privacy and data protection-related issues across the world.[6]

Further, the Mozilla Foundation's Data Futures Lab serves as an experimental space for instigating new approaches to data stewardship challenges. It provides funding, scaffolding for collaboration, convening around emerging ideas, and a place to workshop approaches to data stewardship which give greater control and agency to people. It has conducted and commissioned original research[7] on alternative models of data governance and is providing support[8] to organizations implementing such new approaches through its Prototype Fund and its Infrastructure fund.

Our response will primarily focus on the potential for the UK's consultation to provide clarity on how the UK government can enable more effective forms of 'data stewardship.' We believe that many products and services currently use an extractive model of data governance – i.e., the individual gives up data and the value of that data stays squarely with the provider of the service or product. The status quo does not sufficiently enable data subjects to exercise their rights and benefit from the use of their own data. Therefore, policymakers globally are examining the internet ecosystem through a data lens, not just focusing on platforms or specific products. We believe this consultation provides ample opportunity for the UK government to carry out a similar exercise for a more robust, rights-respecting and future-proof data governance regime.

Data Protection and Individuals' Control Over Their Data Should Remain the Cornerstones of New Legislation

Without sufficient legal safeguards for privacy protections, policies promoting data sharing run the risk of causing substantial harm.

Increased data sharing and re-use of data have great potential to spark innovation and create value for consumers and the public at large. Still, as long as human data is involved, risks remain. Therefore, data privacy should be the bedrock of any law promoting data sharing and increased processing. In principle, the **control over their data should lie with data subjects**, even if data collectors or third parties could make productive use of it or act on behalf of data subjects to facilitate the exercise of their rights.

The key underlying principles of of any data protection regulation should include:

- **Informed consumers:** Information should be shared in accessible ways that are transparent and benefit the user as to how their data is used.
- **Empowered consumers:** Users should be in control of their data and data-mediated experiences, including strong legal protections around informed consent that

[6] Open Policy & Advocacy – Privacy, https://blog.mozilla.org/netpolicy/category/privacy/
[7] Data Futures Lab – Lab Research, https://foundation.mozilla.org/de/data-futures-lab/learning/
[8] Data Futures Lab – Grantmaking, https://foundation.mozilla.org/de/data-futures-lab/grantmaking/

meaningfully enables agency and individual choice while accounting for the unique role played by data stewards.
- **Strong security:** Strong security controls and practices should be in place to responsibly protect consumer data.
- **Limited data:** Data collection should be limited to what is necessary and delivers value.

Mozilla has long advocated for companies to apply this approach through our Lean Data Practices methodology[9] and we apply them to our own products through our Data Privacy Principles.[10]

The EU's General Data Protection Regulation (GDPR) maintains a high standard in this regard and should continue to serve as a benchmark while accounting for the UK's desire to make adjustments where it believes the GDPR falls short in adequately protecting individuals' (and groups') privacy and other rights.

At the same time, regulators should **consider how data protection rules can harness the potential of data stewardship and new models of data governance**, e.g. by including provisions allowing for the delegation of consent to third parties in some clearly delineated circumstances. Further, even when public policy promotes the re-use of data or the increased flow of data, this **should not undermine the foundations of privacy, transparency and accountability** in the collection, processing, and sharing of data.

Alternative Models of Data Governance Can Help Shift Power

Novel approaches to data governance hold much promise, but there are many conditions to be met for this promise to be realized.

Alternative data governance is a nascent field and for most of these new models of data governance, first experiments are only getting underway now. As highlighted by the research conducted and commissioned by the Mozilla Foundation's Data Futures Lab, these alternative and oftentimes novel models can be clustered in, most notably, the following (overlapping) categories of data intermediaries:[11]

- Data Cooperatives
- Data Commons
- Data Collaboratives
- Data Trusts
- Data Fiduciaries

[9] Lean Data Practices, https://leandatapractices.com
[10] Data Privacy Principles.
https://www.mozilla.org/privacy/principles
[11] What Does it Mean? Shifting Power Through Data Governance,
https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/

- Indigenous Data Sovereignty
- Data Marketplaces

Such models have the potential to shift control and value creation back towards data subjects and communities, for example by giving people a greater say in how decisions are made regarding the use of their data, helping them with enforcing their data rights, enabling the creation of intermediary entities that facilitate sharing between different entities etc. However, even when such initiatives are well-intended, **it is not a given that they will succeed in empowering people vis-à-vis data collectors and processors** and in providing them with more agency and control.

In any case, considerable work will need to be done to **ensure that they don't duplicate the existing systemic problems of today –** or create new ones of similar proportion – and instead pay due attention to the following considerations:

- **Consent:** As raised in Question 1.7.2. on the role of consent for data intermediaries, we believe that true data stewardship should always be rooted in consent granted by data subjects, without exception or derogation. To rely instead on the benevolence of an intermediary is to invite new risks and conflicts of interest to arise and no suitable model of governance. Further, individual consent is often insufficient as the harms of data collection and use easily extend beyond the individual the data is about. Collective participation in decision making, for instance through panels or voting, would allow data subjects to together decide what needs to happen with the data or if data should be collected at all.

- **Security:** Minimum security standards and best practices from traditional data protection law must continue to apply to the data (and to stewards) at all times. Additionally, this necessitates high levels of data security and a minimum standard of data management – including curbing the risks of creating centralized data infrastructures, which could become attractive targets for malicious actors or aggravate the harmful effects of data leakage or other security incidents.

- **Trust:** Further, new models of data governance need to be embedded in appropriate governance and oversight structures themselves. Only by putting in place mechanisms and structures that ensure that, for example, new intermediaries act in the best interest of data subjects and communities will genuine trust in alternative data governance models and new data intermediaries be created. This could, for example, include regulatory approval requirements or certification schemes for new intermediaries. In the absence of such robust governance, new approaches run the risk of merely obfuscating existing structures of power and abuse/misuse by giving them a new guise.

- **Legal context:** There are a range of legal complexities to consider in the design and implementation of alternative data governance models, from cross-jurisdictional

challenges to consent models to practical implementation. For example, how would data trusts legally interact? To what extent must organizations with direct relationships with individuals honor requests from third parties purporting to act on behalf of the individual? How does this factor into existing paradigms of data security, confidentiality and contractual privity and waiver? To which degree do existing data protection rules inhibit the roll-out of new models, e.g. by precluding the delegation of consent to third parties acting in the interest of data subjects? Are there legal imperatives to ensure purpose limitation when data is collected? Most importantly, on accountability, are there clear (legal) paths to hold stewards accountable for their actions?

- **Transparency:** We believe that one of the most meaningful ways to enable agency in an increasingly complex ecosystem is transparency. When it comes to models of collective data governance, enabling auditable records of interactions with data – say in the form of secure, immutable logs – can be an effective way to improve trust, enable accountability and empower users when done in a privacy preserving manner. The principle of notice is also a measure of transparency that is crucial to enable agency – intermediaries must be held accountable for properly describing what data they handle, how they handle it, who it is shared with etc.

- **Inclusiveness:** Finally, it should be ensured that there are low barriers to use as to prevent the benefits of participation in such a scheme do not only accrue, for example, to those with high digital literacy and an already better ability to safeguard their interests online – therefore increasing existing digital inequalities.

In seeking to promote beneficial new models of data governance, governments need to **manage the balancing act between facilitating experimentation to create an evidence base and adopting too myopic a vision for what ends such models should achieve**. To identify the most promising options both with regard to data governance models and with regard to the necessary regulatory enablers and guardrails accompanying these, experimentation is needed.

Specifically, in response to Question Q1.7.1, the government has a role to play in this and can become an important catalyst in challenging the existing and oftentimes extractive paradigm of data governance. For this purpose, governments should become active themselves: by funding prototypes – especially in the public domain - by supporting public research, by itself becoming a steward of people's data where appropriate as well as applying Lean Data Practices to its own collection and handling of data, and by assuming the role of a regulatory enabler and watchdog. In doing so, they should always heed the principles outlined above and ensure that this is the case across the entire ecosystem of data intermediaries as well.

At the same time, public policy must be **guided by a clear vision of what values[12] and outcomes alternative data governance optimizes for** beyond the high-level goals of strengthening agency and control and re-aligning economic value creation with consumers' interests.

Collective Rights Could Complement Individual Data Rights

Individual data rights can be a means to correct harms and power asymmetries in the data economy, but some are better addressed through collective mechanisms. Oftentimes, data does not only concern an individual but also a group of individuals. For instance, a main purpose and added value of collecting individual data for many personalized services in the digital economy increasingly is to define relevant group categories, which subsequently increase the collector's capacity to develop models to predict and sometimes change behavior of others based on relevant population features they share with that individual. In other words, significant **economic value is created from the inferences drawn from our interaction with others**.

At the same time, the insights gained from such collective data rights based practices can also lead to **new categories of inferred harms** – where the individual is inferred to be part of a group or category of people but the person whose data is used is not harmed. In these situations data protection often doesn't provide meaningful redress mechanisms. Hence, **new legislation should take an expanded account of the collective interests and harms at stake here**. For example, data intermediaries could be authorised to exercise data rights on the behalf of (groups of) individuals to take into account this collective harm.

Data Sharing is Best Encouraged via Incentives and Legal Protections

Public authorities should **create incentives** for and **enable data sharing** by, for example, encouraging voluntary standardization activities (such as those around templates, minimum security specifications, collating best practices etc.) and identifying means to provide the necessary legal mandates that provide necessary protections for consumers and certainty to the private sector at a high baseline.

In this context, rather than imposing blanket measures to open up datasets, the government should conduct an exercise to **identify those aggregate and anonymised datasets that would be most valuable** to nascent businesses and consumers. In imposing such a mandate, authorities would also need to ensure that access to data is not abused by third parties, that individuals' and companies' data remains secure, and that intellectual property and trade secrets are properly taken into consideration.

[12] Data Futures Lab Glossary,
https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/

There is potential value in data sharing, for example, some companies may have data sets the value of which, if shared with other companies or the public, could raise collective innovation in key technologies or collective understanding of key public issues. However, several important questions would need to be explored, including how this could be done in ways that protect individual privacy and agency over data; in what situations this would apply; and how this would be insulated from abuse by governments given that the power to mandate a company to turn over personal data is extraordinary and in many cases governed under specific legal processes and safeguards to protect against abuse.