GOVERNMENT OF
THE UNITED KINGDOM

3rd May 2029

Government Response to the ad hoc Select Committee of the House of Lords on the 29th February Data Losses

By Phil Booth

Introduction

The Government is grateful for the Committee's comprehensive inquiry dating back to the mass breach of UK citizens' data on 29th February and subsequent events. The new Government believes that everyone living in the UK must know how data about them is accessed and used.[1] Such information is indeed necessary for people to be able to make the informed choices to which everyone has a right.[2]

Respecting choice has long been essential for public confidence in services, no more so than now, as we collectively seek to rebuild the trust that was shattered when bulk personal datasets[3] – vast quantities of citizens' data – were left unprotected on the internet[4] on February 29th.

1. https://medconfidential.org/2014/what-is-a-data-usage-report/
2. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
3. https://en.wikipedia.org/wiki/Bulk_personal_datasets
4. https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/
5. https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence/national-data-strategy-open-call-for-evidence

The confusion and uncertainty of previous Governments on data is self-evident in many of the quotations cited by the Committee, including:

"...the term 'data' is intended to be understood broadly and refers to all kinds of data unless otherwise specified – for example, covering both personal and non-personal data, information that is stored both digitally and non-digitally, and data used for various purposes, e.g. data about people, data about performance, government data, content data and so on"[5]

Previous Governments' attitudes towards, and treatment of, citizens' data cannot be summarised any more clearly than by Baroness Gracey's frustration in oral evidence:

> "Did you believe the law and your public task allowed you to do anything you wanted with data covering the entire population?"

While this Government cannot assist the Committee on that specific unanswered question, it typifies the situation we inherited. This statement from a previous administration remains timeless:

> "We have … security systems, we are updating those security systems, but we will look in detail at how they are functioning in the wake of what has happened this week. But I will stress that while the systems are one thing, the people who operate them are key … The human factor is the decisive one."[6]

This Government recognises the fundamental truth that personal data is data about people who can come to *real harm* – especially when a contractor at the end of an outsourcing supply chain,[7] constrained by austerity and working to tight deadlines within unprecedented administrative complexity, inadvertently creates a single point of insecurity, having forgotten leap years exist.

Fairness and Justice

Following the previous administration's multiple losses at Judicial Review, we accept and actively agree with the Committee that the principle of fairness and justice must apply to all users of digital services, and to all digital decision-making.

The Government will enshrine into law the requirement for all public bodies to comply with new statutory definitions of "vulnerability" and "fairness" – definitions capable of being operationalised empirically, as recommended by the Committee – and, effective immediately, will require all public services to provide evidence demonstrating the compliance of the data architecture of every programme they deliver in a published Data Protection Impact Assessment.

While previous Governments may have believed harms could not be demonstrated if they refused to collect evidence, it is now beyond question that such evidence will be collected anyway.[8] Evidence collected demonstrates harm. We recognise the Committee's suggestion that evidence must be collected, and this administration will do so – but only Parliament can write the laws binding future Governments.

The flow of claims for technology 'ethics and innovations' by 'centres' and 'new institutions' that were anything but privacy-enhancing have been shown to be little more than hype for headlines at the expense of the citizen, and 'governance' by those whose goals are not in the public interest.

6. Q14, House of Commons Foreign Affairs Committee, Oral evidence: FCO secure communications and handling of classified information, HC 2541, Wednesday 10 July 2019. Timestamp: 13:13:13 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/foreign-affairs-committee/fco-secure-communications-and-handling-of-classified-information/oral/103681.html
7. 'Boeing's 737 Max Software Outsourced to $9-an-Hour Engineers', Bloomberg, June 2019: https://www.bloomberg.com/news/articles/2019-06-28/boeing-s-737-max-software-outsourced-to-9-an-hour-engineers
8. https://www.jcwi.org.uk/passport-please

History repeats itself

Distractions around the 'ownership' of personal data only exacerbated the damage to our citizens and our country. This Government therefore mandates a 'verified attributes-first' approach to identity assurance throughout the public sector. Data minimisation is no longer a compliance goal, but a necessity. The requirement of previous administrations that all analytics must have a profit-driven "industrial component" under the euphemism of "deliverability and scalability" will no longer be hidden from the public.

All services predicated upon such approaches will be fully audited and re-engineered according to independently overseen Privacy-by Design principles. Linked individual-level data, rich in detail, is highly identifiable; while using such data securely is entirely necessary, proper handling does not render anything anonymous.

Purpose limitation and lawfulness are critical components of each one of the UK's Data Protection Acts, from 1984 to 1998 to 2018 to 2024.[9] They have been ignored at the peril of our citizens.

The Government welcomes the National Audit Office's recent report, 'Ten Years of Challenges in Using Data Across Government', which updates the 2019 report of a similar name.[10] As the NAO makes clear in its report, had steps already known to be necessary been taken in 2019 – or indeed in 1999[11] – this foreseen sequence of failure upon failure[12], response compounding error, would not have been so catastrophic to public confidence and public trust.

When service owners do not listen

When selections from the official archive of phone call recordings were published by the media following the February 29th breach,[13] the "brutal inhumanity" of the previous Government's policy was made plain.[14] The journalism placing audio from DWP helplines next to photographs of the victims and details of how they died was described as "haunting". We agree with the Committee that the episode was an "indelible stain on Her Majesty's Government".

It is impossible to deny that the harms of digital services are real when one hears those calls; past Ministers and senior officials simply did not listen.

The Government has already begun implementing the Committee's recommendation that Permanent Secretaries, Senior Responsible Owners, and Secretaries of State should sit in on at least one hour per year each of user research and helpline calls, though it was unable to ensure these calls were randomly selected and not carefully screened. We invite and encourage future work by subsequent Committees to consider how institutional denial insulates decision makers from the actual and harmful effects of their choices.[15]

Parliament itself should scrutinise practice, given the very different approaches of different Governments over the last decade or more.

The interim publication of '(Nearly) Ten Years Touring The Monster Factory', a report by medConfidential, documents and details failures throughout the past decade – failures which led to the choices the Committee describes as "catastrophic" for both the country and citizens alike. This Government is cooperating in advance of the final report.

The Government recognises members of the public care deeply about the quality of their public services; that they are funded appropriately, that they are run competently, and that they are available to all as needed. It has been many years since the public made any real distinction between 'digital' and 'non-digital' services – they rightly expect things to just work safely.

Harms

The harms of data use, abuse and misuse are not equally distributed – those reading this document are amongst the least likely to be affected. Those who are affected will likely be amongst the most vulnerable – whether through possessing characteristics protected by the Equality Act, through fear or distress, or through circumstance or misfortune.

The Committee argued, with hindsight, that the primary folly of the 2010-2015 era of Digital Government turned out to be its presumed benevolence – that 'digital' was, and would only ever be, a force for good.

The years 2016 and beyond revealed the flaws in that approach – 'thoughts and prayers' were insufficient. While lists of principles and frameworks were popular, these were only meaningful when transparently operationalised with independently-designed metrics to evidence compliance. 'Digital' can be more effective at manifesting misery than it ever was for increasing engagement – much as was proved to be the case during that period, for both empowerment and democracy.

The Government recognises it is by and large the Courts and the Justice system, led by those with an innate sense of justice, which ensures the equality of all under the law is maintained. Until every public body has understood and fully respects that principle in every aspect of its digital policy and practice, they will continue to lose Judicial Reviews in front of judges who do.[16]

---

9. http://dataprotector.blogspot.com/2017/10/briefing-paper-to-peers-in-advance-of.html
10. https://www.nao.org.uk/report/challenges-in-using-data-across-government/
11. http://danbarrett.posthaven.com/data-20-years-of-hurt
12. https://twitter.com/GavinFreeguard/status/1147074348680921088
13. https://twitter.com/NetworkString/status/1156291545718558722
14. https://twitter.com/WEDFglobal/status/1149869371113820161
15. https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma- working-conditions-arizona
16. https://civilresolutionbc.ca

Choices

It is the policy of this Government that all uses of data by public bodies can be seen by the citizens represented within that data – on NHS.UK for their NHS data, and GOV.UK for everything else. Where choices exist about how data is used, the effects of those choices can be clear – and it is equally clear when (and why) those choices do not apply.

The Government notes the Committee's conclusion that expansive reliance on limited exceptions is entirely inappropriate, and accepts its recommendation that the use of such exceptions be discontinued, recognising this is a legacy approach from four decades ago, in a world that has changed immeasurably during that period. We will shortly consult on the closure of remaining loopholes.

That previous administrations sold the personal data of patients who had opted out of the use of their data for purposes other than their individual care was *prima facie* wrong, and the harms to those people are not the hypothesised risks decried by commercial advocates at the time.

The harms cited by the Committee, and the harms cited by other Committee reports and official inquiries are real, they are evidenced, and were entirely predictable. They were also predict*ed*. Predictions and possibilities only matter when Government chooses to listen – the previous administration did not, and to quote the Committee, "the most vulnerable of innocent citizens paid the price".

We agree with the Committee that the consequences of the February 29th breach and some of the responses to it have threatened the intrinsic values and principles of the UK, and that it is right that Government addresses these issues as a matter of priority. This detailed and considered inquiry has made a valuable contribution to the public debate, and the evidence, conclusions and recommendations of many Inquiries in Parliament have enabled this Government to draw on a wide stakeholder and evidence base in considering how best to tackle these issues.

The Government will bring forward legislation to ensure that loopholes in the Data Protection Act are closed. 'Public task' must mean demonstrating compliance with the rule of law, and citizens must be able to know how data about them is used,[17] absent an unambiguous statutory requirement otherwise, e.g. for National Security, Public Health, or Official Statistical purposes. The convenience of user access to comprehensive administrative data was placed above real harms to families who believed they had protected themselves from official data mistakes and misuse – only to find that Government had ignored the choices they had made, and that they had become victims anyway[18].

Sir Bonar Neville-Kingdom III GCB
His Majesty's Government

17. https://medconfidential.org/2015/implementing-data-usage-reports/#gdur
18. https://www.gov.uk/government/news/data-driven-innovation-and-meeting-patients-reasonable-expectations-about-data-use

Radical Visions of Future Government

nesta