Annex 8 – Government ‘Super-Apps’

In this annex, we explore how two public sector "super apps" have emerged: the Gov.UK Black app, and the NHS (blue) app. We'll examine their rise to prominence and the predictable consequences that follow. By using simple examples for each issue, we can better understand both apps' incentives and the consequences of current decision making structures.

The forthcoming Gov.UK app is a prime example of how government services are being digitized. This "black app" aims to provide citizens with easy access to various public sector services, such as renewing passports or checking benefits entitlements. With its user-friendly interface and streamlined processes, the effect will allow Government to read from the sensors on a device in every citizen’s pocket.

The concept of a "super app" may be unfamiliar outside China, where WeChat has become an integral part of daily life. This popular platform allows users to perform various tasks, and is so popular it can be used to pay in some chinese restaurants in the UK. Superapps are largely blocked by Apple and Google app store rules, so effectively don’t otherwise exist, but is what Elon Musk wanted to do with Twitter.

One of the precursors to our work on the data flows of Universal Credit was a piece for NESTA on the consequences of our current behaviours of governance and data. The coming election will likely form the government that was kicked out of office after the tech catastrophe setting the scene for the report. The rise of large tech doing government’s bidding, and the inevitable catastrophe was depressingly prescient – Post Office Horizon, UC, NHS/Palantir from the UK, or robodebts from Australia, or the Netherlands, or …

Everything we have talked about here for the NHS app will happen with clogs on for the gov.uk black app. When citizens are effectively forced to install the app, they should then disable background refresh and prohibit it from notifications, so the app runs when you open it, and doesn’t when you close it.

It is unclear what a sustainable and good (or even competent) process here looks like, or can be in the face of a Secretary of State who wants everyone’s device to go *ping* about his new pet project. 1984 with wireless telescreens and modern microtargeting.

Table of Contents

Annex 8 – Government ‘Super-Apps’ 1
Table of Contents 2
1. The Black App 3
2. ‘JFDI’ 4
3. Intrusive data in the Department of Health in England 5
4. “One Login” for Government 6
5. Notifications 7
    Notification choices 7
    Sending notifications 8
    6. Scope for necessary future work: Bad news / Timing of notifications 9
7. Sensors, tracking, and derivable data 10
    Sensor access is not always a choice 10
    For or against the user of the device? 11
8. Service users see the service they receive 13
9. Prosecution Policies and Unanswered Rule of Law Questions 14
    Continuous change and consequences for prosecutions / tribunals? 15
    Rule of Law vs Departmental Stovepipes 16

1. The Black App

The description of the vision of digital government in 2013 was ‘not appy’ but websites. A decade later, the culture of government is apps and code running on your device not on Government’s servers.

To adopt this new approach, there needs to be a thorough reevaluation of what government can and should do. Unfortunately, such an assessment is not being conducted. However, if we were to condense this idea into a single sentence, it would resemble the dystopian scenario depicted in George Orwell's "1984," where citizens are constantly monitored, with wireless telescreens and modern microtargeting.

Once a feature is enabled for one purpose, such as checking if your current fishing licence is valid where you are standing, it can be used by any part of Government that uses the gov.uk app. This means that other government departments and agencies wanting sensor data from the Black app may not need to ask the user before they access those sensors.

The technology exists for a gov.uk app to wake up at 4am through a silent notification, listing what wifi it can see and finding its location. It could even tell whether you spent the night somewhere other than your home (and where) when matched with commercially available databases. This raises concerns about how many nights you spend in the country, which would be of interest to HMRC, while DWP might feel obliged to know, and HO would likely use it in their traditionally racist way.

It could be argued that User Interface and Experience teams can offer good service design with only positive design patterns, but without a robust way of persuading new Ministers not to copy dark patterns from their personal apps into government superapps, these apps will inevitably degrade because Ministers often say JFDI.

2. ‘JFDI’

When a Minister says “JFDI” on their pet project in the App (gov.uk Black or NHS Blue), the civil service will implement it, even if it is harmful to the app itself, because Ministers Decide.

If the Secretary of State for Health wants their smiling face to be the splash screen for the NHS App, they can say “JFDI” and NHS England will do it as a priority.[1]

Digital gives great power to Ministers to intervene in your home life and that of your children in the same way Uber micro-monitors the time of their ~~gig workers~~ staff or how schools now monitor students both at school and at home.

Those who wish to claim their 30 hours of free childcare are made to jump through bureaucratic hoops every three months[2] in order to reduce the number of people who take up the “free” service and to minimise cost to the Treasury. The costs to the citizen are not considered, and possibly not calculated[3] by Government. Such calculations are entirely possible.

The development processes of digital apps do give civil society the ability to see into that process, even if the organisations refuse to listen when questions are asked prior to launch. We cover that topic in Annex 8B and the final (legal) sections here.

With NHS App harms, ministers said JFDI and insisted that features were rolled out ignoring the consequential risk to patients. Yes, registering with a GP should be easier, and the Department of Health in England argue that if someone is maliciously registered on the other side of the country, they can now move back just as easily, but re-registering someone with a GP outside their current ICS means all their repeat prescriptions get cancelled, all their waiting list positions are lost, and mental health care goes away. Because protections had to be implemented by GPs processing the registrations, and NHS England did not wish to properly engage with them given their rush to roll out a political priority, on the political schedule, so it deployed without meaningful protections in place. None of those things are easily fixable, even if they had the half billion pound budget available for Palantir in the Department of Health in England (who made similar decisions for similar reasons).

Politicians naturally believe that their own desires are in everyone’s best interest because they themselves want them. That assumption applies equally well to Wes Streeting’s wants for the NHS App just as much as it does to Michelle Mone on PPE procurement.

[1] These NHS England slides don’t talk about “the JFDIs” but they clearly exist, and clearly have to be done. The video of the presentation gives a little more context.

[2] https://twitter.com/blangry/status/1687013629915205632?s=20

[3] https://x.com/tomskitomski/status/1687017062978207744?s=20

3. Intrusive data in the Department of Health in England

Traditionally health has had far more data on individuals than other areas of Government, but the Black App allows highly intrusive monitoring of everyone via their devices. The less Government took from the pandemic is they want the same intrusion as the NHS.

Governments use available tools to advance their aims – that isn't necessarily always a positive thing.

Palantir isn't particularly unique or special, despite cultivating a reputation as cartoon villains to sell their products. What sets them apart is their lobbying efforts to maintain that reputation and boost their share price. They'll do whatever their customers want, just like civil servants will follow ministerial orders, and apps will cater to what ministers demand. If it came to collecting data from apps to monitor women's menstrual cycles, where in Texas, Tehran, or Tyneside, Palantir do what their customers wish.

If Wes Streeting wants his face on the splash screen for the NHS App, "JFDI" is NHS England's policy. Rishi Sunak called the election before his face can go on the splash screen for the Black app, irrespective of public trust, but he would have if no10 had known to ask.

Two decades ago, catastrophically screwing up at national scale required losing a compact disc[4] – it was almost impossible for a Minister or civil servant to have a direct immediate effect on millions of people. Digital offers new opportunities, as Hawaii found out in 2018.[5]

A mishandled merge, in a system designed to hide bad news, results in irrevocable harm for as many people as are affected (that the Home Office didn't bother to count). Right to live checks affect everyone – including British citizens – and there is no reason the Home Office will care any more when they screw up your record as when they screw up someone else's.

The separation of health records present barriers to catastrophic damage, but if the political consensus to merge to one database of everything to be owned by the Department of Health in England moves closer, the greater risk comes to government medical records. In such a scenario, individuals wouldn't be able to dispute medical notes recorded centrally by the NHS or challenge any inaccuracies, as these records would effectively become government property – something that Labour views with concern, implying that "ours" could come to mean "government's".

They'll want to sell the whole thing, linking all the data together and protecting only the unknown magic number that does the linking by replacing it with a different one. However, if you had a kidney removed in a particular week at a particular hospital because you publicly thanked the NHS for treating you, you can read Wes Streeting's entire medical history - including things he would rather weren't public. There's no need to break the Maginot Line of pseudonymisation that the Department of Health in England relies on exclusively to protect data as they sell it, even if people have tried to object to that sale.

[4] https://en.wikipedia.org/wiki/Loss_of_United_Kingdom_child_benefit_data_(2007)
[5] https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert

There is no health data that will not be affected, and there is no data that will not follow afterwards.

Those who "go private" entirely for their care will find that their data is copied anyway. The implants registry will track all people and those implants, along with the type of surgery that led to that implant and the diagnosis it implies. This is without considering a single healthcare record where public and private entities (and their AIs) can read and write to "offer" you care, replacing the notion of a family doctor who expects to be around to see your kids grow up. The 2024 instructions on the practice of medical reason for tory campaign reasons show any boundaries are entirely at the whim of the Department of Health in England.

There is always demand for more, and just because they can’t get something today, they will keep trying tomorrow. The system wants what the system wants. And the new Government will be offered shiny narratives for sharing ever more; rule of law be damned.

4. “One Login” for Government

The "One Login" service requires users to provide working email addresses and phone numbers for every account. To access government services, individuals will need to verify their identity using a photograph and official ID. This setup raises concerns about unrestricted facial recognition data being shared across government agencies without safeguards in place.

Furthermore, the verification process involves taking a selfie to claim Universal Credit (UC), with no statutory protections against matching or storing this data for future use. While it's unclear whether this information is stored in an easily analyzable format, there are concerns about potential misuse if Ministers choose to do so. It would only need a political decision to require everyone on UC to revalidate their photo and the Blackapp could insist on GPS and camera access to take the photo to satisfy the process. “BeReal” as a policy proposal.

If UC was built to an image assumed by IDS, and gov gateway was quietly rebuilt embedding the elitist assumptions of Treasury and HMRC,[6] then institutional racism and dismissal of good governance typical of the Home Office is embodied in One Login.

When a future political assessment says those who are politically salient all have the black app, the expectation of having ID in the App that ‘everyone has’ will turn the Black app into the electronic ID card. ~~Papers~~ Apps please!

We return to the consequences of One Login in the final section on the Rule of Law.

[6] https://twitter.com/yasgeorgiou/status/1681414523788378129?s=

5. Notifications[7]

> “Patients will be sent NHS phone alerts urging them to join clinical trials under Labour plans to massively expand the use of health data.” - The Times

When everything is a priority, nothing is a priority.

Every part of the NHS thinks they should be able to send notifications, because each department is convinced that what they're doing at any given moment is the most important thing. It's all about user needs, not system needs. The same will likely hold true for Government Departments,[8] and then people will turn the notifications off because they’ll enshittify down to junk, which will further increase the pressure to send even more junk.

Notification choices

Your smartphone has a small number of categories of notifications[9] – critical (“blood glucose very low; eat to not die”), time sensitive (“leave early for your meeting because traffic is bad”), active (“you have a meeting in 10 minutes”), and passive (“something in your calendar changed for next week”) – all delivered through the same channel, and with the user having (some) control over them.

All alert mechanisms will get abused for commercial reasons, or other priorities. Apple themselves are notorious for ignoring the rules and doing what they wish. Government departments (and the NHS) assume they can do the same.

Commercial apps are incentivised to promote notifications, increasing the importance for commercial reasons, but not quite enough that too many users will turn them all off.

Once notifications are turned off for an app, or turned down, all notifications for that app get turned off.

It is inevitable that apps will find ways to justify having "critical" alert permission, and then there will be pressure to misuse them. Just as Public Health England was unable to prioritize different public health priorities, Departments will have their own silos which believe their own objectives are the most important thing for every citizen.

And then people will turn the notifications off because they’ll enshittify down to junk, which will further increase the pressure to send even more junk.

[7] NHS Notify is outside the scope of this document, but a set of questions are published here: https://medconfidential.org/wp-content/uploads/2024/06/2024-05-23-Notify-NHS.pdf

[8] https://x.com/rachelcoldicutt/status/1776566645537857902 or https://x.com/rachelcoldicutt/status/1798606480989651242 or many, many other examples…

[9] https://developer.apple.com/design/human-interface-guidelines/managing-notifications; Android has similar.

Sending notifications

Notifications and sensors interact – when an app receives a push notification, it doesn't have to show something on screen, but can read sensors it has access to, including location and send data back to the servers.

Prioritisation processes

Politicians prioritised showing waiting times in the NHS app, but the waiting times shown aren't the real figures due to definitional games to fiddle the figures.

As sole controller of the NHS app, the Department of Health in England is constitutionally and politically entirely incapable of managing the prioritisation process. Individual staff may be able to do so for some period of time, but individual staff capable of prioritising user needs* eventually get moved on and replaced with sycophants. NHS England had a prioritisation process for the app, and then abandoned that process because it didn't suit the administrative fiefdoms of the institution.

Everyone will think that their remit deserves notifications, and while some will get lost in the process, there will be far more junk than there should be. For example, every NHS research project will think that they need to nudge users ever more into participating in research, and the notifications will become increasingly annoying, eventually being silenced. Even if a good decision-making process is established today, those wanting their own exception will return tomorrow, being blatantly opportunistic to get whatever they want, regardless of user needs*.

There are also adjacent abuses of power in the name of "efficiency" meaning less work for NHS England. NHS England tells service providers who have their own apps that they are prohibited from sending notification to *their* users in their own app, until after the NHS app has already sent their notification to the user. NHS England again lowers the standard deviation by making everyone the lowest common denominator: themselves. This is the natural consequence of a write-round policy common to both apps.

The rest of Government won't be any better when the black app comes in. In fact, it will be worse because some part of the Home Office will take charge of sending notifications to certain users of the app – and you know how that usually goes.

While we primarily focus on sending notifications, there's also a political decision made by England's Department of Health not to notify people. The NHS England requirements for GP Connect - widely abused for looking up GP records from hospitals – require providers to show data subjects when and where their record has been accessed. However, NHS England doesn't offer such a mechanism in the NHS app. The culture and practice of England's Department of Health is that if people can't see the harms, they'll never have to deal with the fact that their policy choices cause them.

6. Scope for necessary future work: Bad news / Timing of notifications

There is also the question of when individuals want to see they have new information.

Consider a patient receiving a new terminal cancer diagnosis. A letter sent to their GP is made visible to the patient upon receipt (as per DHSC mandate), potentially viewed after services close on Friday night. What does 'the system' expect the patient to do? What do they think the patient should do? How has/will the content of that letter changed as a result?

Some patients will want to know instantly, if you're stressing about your blood test results, going ding might be the ideal option? if you're not thinking about it, and alone, maybe looking at a time of your choosing later may be better? But maybe not when tipsy on a friday night and support services are closed? There is no obviously right answer.

This question is not unique to the NHS app, or the black app – when should a court/CPS/ tell a rape victim that the case against the defendent has been dropped? Some want to know instantly, before they see it via other channels, others would want support around them. What is the UI/UX for that?

7. Sensors, tracking, and derivable data

The black app: 1984 with wireless telescreens, and modern microtargeting

Sensors are a necessary part of what makes smartphones intelligent and interactive. These tiny devices allow your phone to perceive its environment, respond to touch, light, sound, and motion. By detecting changes in their surroundings, sensors enable features like gesture recognition, facial detection, and ambient awareness.

In the age of apps, sensors have become an essential component of modern smartphone technology. iOS from Apple has relatively specific permissions, while Android from Google is more general and open.

Sensors create readings, readings are stored on your device, from where they can be accessed, analysed, and be copied elsewhere by apps (which can copy both the readings themselves and the outputs of the analyses).

The granting of permission needs only be justifiable by one part of the app for that data to be available to all parts of the app. The user is often not given any choice. If you give access to the app to access your photo library to upload a photo of something, if the app can read all photos, it can upload all photos. If it can see location at any time, it can see location at any time.

The full list of sensors in any device is dependent on the make and model of the device, but the readings that can flow to an app includes location (both GPS, but also the wifi networks you can see[10]), camera and photo archive, balance and orientation (compass and gyroscope), accelerometers for speed of moving, barometers to tell when you're climbing stairs, the microphone, and beyond.[11]

Sensor access is not always a choice

There will always be good reasons for access to everything. If you want to send a photo to your doctor via the NHS app, or photo a document to send it to DWP via the black app, then photo access can be useful. Whether that's just some photos or all photos is a decision for the developers paid by gov.uk. If the Home Office suspects you of an immigration crime, they may argue they *should* be able to access any photos that the gov.uk app has access to. It's their job to argue that, and it's the Cabinet Office's job to say no, but they have to win every time.

The Home Office believes that it should be able to rummage around in the medical records of all women in the country to see signs of sham marriages in expressions of sexual dissatisfaction or other signals. Smart devices can see some of the physiological

[10] Which can be matched to lists from commercial sources – wifi access points tend not to move very much.
[11] The internet has longer lists/descriptions, such as: https://www.gotechtor.com/smartphone-sensors/

consequences of sexual acts, and enough context from the phone to assess whether it was at home. The Home Office would argue it was the obligation of the Black App to collect that data and share it with the Home Office. If your phone is travelling too quickly down a motorway, it knows that you are speeding. The examples are almost endless.

DWP will want to bully claimants into handing over barometer/accelerometer data to the app for the longest period possible, and then punish them for the time someone else carried their phone over to a charger. Those who claim to be searching for work may be forced to disclose their ScreenTime[12] reports of how much time they actually spent scrolling through DWP Find A Job, which is the measurable version of the UC expectation to "look for work".

The UK Government has already made one decision that an app should refuse to work at all unless you give it all the permissions it "requests" – the English covid19 tracking app did not work if you had notifications disabled; the Scottish app worked just fine without. The Ukrainian Diia app, upon which the Black App is modelled, restricted access to services if their databases suggested you should have been conscripted but weren't shown as serving. These denials are decisions written into the code of the software, code that the public may not be allowed to see, written by developers who are told to JFDI by Government.

For or against the user of the device?

These sensors can be used for individuals as well as against them.

The NHS Moorfields project with DeepMind showed that a photo of the eye can assess the state of blood vessels of the eye which correspond to the blood vessels in the heart and body. A decade ago that was impossible, in 2018 it required a hospital, in 2024 now requires your optician, but as the camera in the most expensive iPhone gets progressively better, at some point will be good enough to take that photo, and 4 years after that it'll be in every village on the planet in commodity smartphones. Technology marches on.

The NHS app could include a feature to assess lung function – hold the microphone on your chest and breathe – to compare it to yesterday or previous assessments by the app, to tell whether your grandpa should call an ambulance at 4am because he can't breathe, or whether he's fine and should go back to sleep. The NHS has it's own dysfunction in prioritisation – the challenges we cover in Annex 8B are not unique to DWP.

Labour's Wes Streeting argues that if other people give *any* app access to those sensors for whatever purposes they choose, then he should have access to sensors on your device for whatever purpose *he* chooses. The NHS isn't immune to special pleading and outright bullshit. ChelWest Hospital CEO and Palantir-lobbyist Matthew Swindells simultaneously argues that the national Palantir-hosted Federated Data Platform should be able to do anything he wants around 'his' hospital, but the national NHS app shouldn't do things that he doesn't like at all. Narrow special interest lobbying does not need to be coherent in order to be successful.

[12] https://support.apple.com/en-us/108806

The sensors in your average smartphone are becoming good enough to diagnose someone with parkinson's disease,[13] and the similar analyses can suggest how inebriated someone may have been at each point for which data is stored. There will then be a health argument that all available data should be analysed, retroactively, upon a woman giving birth, to see if her child should be checked for foetal alcohol disorders. It's unclear whether that's better than the abject racism of the existing process. It is, of course, entirely in a woman's interest to give such access during her pregnancy so her health professionals have access to data about her and can detect and address any risks early. That the data will also be used against her will not be mentioned by those professionals. No one should be put in such a position.

The data from sensors are run through models, algorithms and AIs, and the outputs stored, or in other cases, all the data is copied to NHS England's Palantir to "run the models centrally" or, probably equally honestly, to monitor people later by looking retroactively at past behaviour. As always, it will be women who bear the brunt, with the ability for the State to monitor their menstrual cycles and micromanage their lives.[14] Care may be denied if access is not granted, the same way Universal Credit makes it very difficult to open a claim via phone (policy says you can, Job Centre practice is to dissuade so far as to make it almost impossible).

A September 2019 edict to put google tracking cookies everywhere on gov.uk floundered on the need to *not* put them on pages where users were told, with force of law, that the information would only be between the user and the service – most notably being statements to online court services where google analytics implemented naively would be a contempt of court by HMG in every single case. The same will be true for gov.uk app analytics, which can hover up every sensor reading that they have the ability to access. DWPs' JobCentre interrogations will potentially have arcane details to ask claimants about – that their device moves more quickly than someone on PIP may be expected to move, or is kept overly charged for someone with mental health conditions.

Endnote: Various pre-release readers commented this section was overly dystopian, then Google/YouTube decided to use sensors to make users stare at their ads.

[13] https://www.nature.com/articles/s41531-023-00497-x
[14] Note to any US readers under a second Donald Trump term: this is not a policy suggestion.

8. Service users see the service they receive

In their “computer says no” reports, The Child Poverty Action Group highlighted the importance of open source to uncover small and nuanced bugs in complex systems like Universal Credit by seeing what it actually does rather than relying on ministerial claims. This transparency would benefit citizens, boost public confidence, promote accountability, but be detrimental for ministers and the Department in the short term

Many UC processes are not automated and rely on manual changes to amounts, which can sometimes be incorrect. In some cases, it's impossible to know for sure what was done when it should have been or wasn't done when it shouldn't have been. As a result, DWP punishes claimants for the mistakes made in these calculations.

Staff of the JobCentre / UC can change people’s funding amounts at will. DWP claims this is only allowed in specific circumstances, but we've seen similar assurances from the Post Office about Fujitsu/Horizon. There are many bugs or unimplemented features in UC that DWP argue allow them to adjust payments arbitrarily; it's unclear whether they do or don't – as much information remains hidden by DWP.

A commitment to truth and integrity can last longer than an institution’s ability to cover up their actions. It is through keeping meticulous records that Alan Bates could show that Horizon had bugs – he kept his own records and worked with others who had the same problem (with less evidence). It also took decades. The task can look thankless and pointless[15] until the time comes.

[15] Some people may do so anyway https://www.thegrocer.co.uk/the-grocer-blog-daily-bread/why-jack-monroe-is-the-grocers-hero-of-the-year/674775.article

9. Prosecution Policies and Unanswered Rule of Law Questions

The Post Office Scandal is the biggest miscarriage of justice in British legal history; the Cabinet Office and Government Digital Service appear to see that as a challenge to beat.

The origin of the whole of our UC work was looking with others at how the rule of law applies around the digital welfare state, and digital services more widely. It is apt that we finish back where we started.

Three 'features' of UC identified by CPAG in their report are 1) the lack of detail in the statements that claimants see, 2) the ability and regular practice of DWP to replace those statements and delete the 'old' ones, and 3) the ability as a 'business need' for DWP staff to make manual changes to the amounts due to claimants, 4) and users routinely end up in the justice system based on the records and decisions of the system. The institution says the institution doesn't do it unless it's appropriate, a toxic combination of the same actions that embedded the Post Office Scandal in Westminster's consciousness. CPAG were talking about Universal Credit, which does the same thing for the same institutional reasons.

DWP will prosecute based on incorrect decisions it made ignoring data it holds and but doesn't tell itself – the left hand doesn't know what the right hand knows and sends people to prison or confiscates their life savings anyway. Staff believe they're satisfying their public task.

The State prosecutes vulnerable people relentlessly based on information submitted (or not) through web forms where the owners bicker about *their* form not being *our* form - "Tell us once" has a long and complicated history across decades in government. It is the easy thing from the citizen's perspective, but the stove pipes of Government largely hated it but advocates so far have just about kept it alive. In a BlackApp world, that will not be enough.

It is DWP's official position that if you don't tell a second bit of DWP the information you have already provided a different bit of DWP, they can prosecute you for fraud. In a Black App environment, it may be that information is provided through different forms both branded gov.uk both accessed via the same username and password in the same app. You will be open to prosecution if you don't fill in the same information twice in a single app running on your device (and in other circumstances, if you do fill in the same information twice, through almost identical forms, you may also be prosecuted for trying to defraud the taxpayer via duplicate claims).

The reason the Post Office scandal came out is because Alan Bates kept his own accounts and could show the Post Office figures were wrong. DWP doesn't encourage or assist UC claimants to keep such receipts,[16] but perhaps there's an equivalent of Alan Bates who has those records for their UC experience, kept because their commitment to truth and integrity can last longer than the State's ability to cover up mistakes.

[16] Some people may do so anyway https://www.thegrocer.co.uk/the-grocer-blog-daily-bread/why-jack-monroe-is-the-grocers-hero-of-the-year/674775.article

Continuous change and consequences for prosecutions / tribunals?

We covered DWP running experiments on users in annex 5, which involved making changes (they say improvements) to the wording of questions and routing at any time for subsets of users.

It is good that DWP improves the system – the best time to improve the wording on a question/workflow was the day it was added, the second best time is now. However, DWP often ignores the fact that the changes have consequences.

No user knows whether they had the “old” or “new” wording, and if a minor tweak is interpreted very differently by users, or just some subset of users, or just one subset of the A/B group, then those users may answer a question honestly but in a way DWP later feels inaccurate and which DWP may prosecute them for fraud. Government UX staff do not act as if their jobs may result in people going to jail; but they may.

With every service being subject to continuous improvement – bugs being identified and fixed – what mechanisms are there in place to identify changes that correct service failures of people not being asked a question clearly? Does anyone check whether those failures can result in prosecution for fraud / dishonesty / theft of the public services / funds they got as a result of answering questions with honesty and integrity. Are the prosecuting authorities told?

Is anyone sitting in jail right now because of a botched UC or gov.uk A/B test?

As argued in Richard Pope’s work on UC, the code and change history should be open source to allow external scrutiny of changes over time. Without that transparency, we are entirely reliant upon DWP to give full and complete disclosure to the prosecuting authorities and to the defence, when it may not have any idea that an “anomaly” had been there at the time the user used that part of the system.

Rule of Law vs Departmental Stovepipes

DWP currently maintains its own presence on the internet, and ‘telling DWP’ is a very clear act, done on the DWP UC website with a DWP UC login. Is that the same when it’s all in the ‘gov.uk app’ via One Login, when there are no visible boundaries at all? This will open many ‘interesting’ questions which should be fully examined and understood before Departments start finding and prosecuting individuals who have a defence that they used the black app as the designers in GDS entirely intended.

In a “one login” and “Black app” environment, a citizen uses gov.uk with their (one) login to notify the Government through a gov.uk branded form of some particular distressing change in their circumstances. They believe they have fulfilled their obligations as an honest upstanding citizen, but a Secretary of State still believes they have not been notified via a different gov.uk branded form accessible via the same gov.uk app with the same username and password, and the citizen is potentially prosecuted for fraud and sent to prison as a result.

When the app was filled in, is it legally reasonable for a citizen to believe they have told a Department information in a form in the app that the same Department directs them to use?

Citizens can be prosecuted and sent to jail for not filling in the same information in two different forms to tell different bits of Government the same thing. In a Black app world, they will both be via the same app and there is no obligation on the app, GDS, or anyone, to ensure the citizen is aware that just because they’ve told gov.uk in one place, they also are legally obliged to tell gov.uk in a second.

More strongly, if you tell the app something through one set of questions, it will be difficult to argue that you did not tell the same app the same thing when another department wants to penalise you for not telling *them* via the same app.

That the Black App is not being built with the Rule of Law (and practices of Departments) in mind rests solely on GDS. The consequences of imprisonment rest solely on the citizen.

Government will prosecute citizens anyway, and potentially make the Post Office Scandal look like a warm up act.