


LEGAL

This article is more than **1 year old**

Bigger, dafter, creepier - Gordon Brown's ID scheme rescue plan

Get the shops to pay for it, *and* catch villains for us...

 [John Lettice](#)

Mon 7 Aug 2006 // 12:23 UTC

ANALYSIS 'Sources' close to Chancellor Gordon Brown are floating plans to finish off ID cards entirely in the UK - although that isn't *quite* how they're putting it. Instead, the advance men for the Prime Minister in waiting are offering a nightmare pitch that harnesses the private sector to implement a total surveillance system while raking in revenue for the Government.

Most of the components of what's being run up the flagpole now have already been suggested by mad wonks, with reference to the Home Office ID project. Future generations of cashpoints and point of sale equipment, they've told us, could cater for biometrics and ID cards, and the widespread use of ID checks in association with financial transactions would combat identity fraud (or credit card theft, as we used to call it before we needed to fiddle the identity fraud figures). People would find themselves (happily, not grudgingly, in this deranged scenario) using their ID card several times a day, and all of those lovely ID checks of the National Identity Register would provide the Government with revenue, and detailed records of everybody's financial transactions and whereabouts.

For example, right back at the start in the consultation document for the entitlement cards scheme (remember that?) we were told: "Existing cards such as loyalty cards issued by retailers could use the entitlement card, saving the cost of producing and distributing cards. Organisations might also be able to make use of cards for internal purposes for example access control to their premises or computer systems."

Harsh realities however have meant that we've only seen glimpses of the weird vision of total security, total surveillance in ID scheme documentation. The idea has still always been there, in the sense that the Identity & Passports Agency is being positioned as the UK's identity gatekeeper within a Government monopoly of ID verification services, but the point where the private sector piles in has always been out there in the middle distance, in some future phase where ID cards had already taken off.

So on hearing what Gordon is allegedly thinking one begins to wonder if perhaps this man skipped watching most of the last series. The proposed "massive expansion" of the project

certainly suggests he's been smoking the biometric crack, and has bought into the notion of single, centralised ID big-time.

Yesterday's *Observer* report details some of the benefits Brown and his team see as deriving from a more extensive and pervasive ID scheme, but gives no indication that they've considered the associated costs or the feasibility of the proposed extensions. It is suggested, for example, that stores could be allowed to "share confidential information with police databases" and that this would mean police "could be alerted instantly when a wanted person used a cash machine or supermarket loyalty card."

Well, how does that work then? Clearly people making point of sale transactions would need as a matter of routine to have their ID checked against a list for... For what? Arrests warrants? All arrest warrants, or just for the more serious crimes? Non-payment of fines? Effectively, once you've made the decision to run the check at POS then the structures you put in place could support enforcement action for a wide range of reasons by any organisation. Note also that when a wanted person is using "a cash machine or loyalty card" the network already *has* a record of their name and the transaction. So you could just as well do the alerting right now if the systems supported it. What they're talking about here is therefore really more a case of using an ID card to verify the cardholder's ID, and bolting on a new deck of state surveillance while they're about it.

We probably shouldn't hold our breath waiting for the civil liberties implications of this to dawn on Gordon, but the complexities and impracticalities of actually doing it will likely come to his attention sooner. How would the check be set up? Would warrants on the police national computer be matched by an automatic flagging of the individual on the NIR? No, because the police don't necessarily want everybody to know who they're looking for, and the 'automagic' linking would be a pig to set up, considering the current state of police systems. What would happen when a fugitive was IDed at POS? Tricky one this - you can't safely alert the checkout operative, or the potentially dangerous terrorist currently buying a kumquat. So it has to be an alert tripped at the NIR level and then a further alert has to go to the police response centre covering the area, then a patrol vehicle has to be alerted... Need we go on? By the time it gets to the response centre you need to have time, location, name and nature of the suspect, and he'll be long gone.

Aside from the obvious technical issues, there's the problem of convincing businesses - what's in it for them? Identity fraud, the Government keeps telling us, is a major concern (but apparently not major enough to warrant the Government measuring it properly) and needs to be fought. Banks, credit card companies and major retailers however aren't automatically going to line up behind 'rock solid ID' *at any cost*, and nor will their customers. Yes, ID fraud is a cost to business and an inconvenience for the victims, but the costs are bearable, and the more security you have in a system, the more inconvenient it's likely to become. So there's a pretty strong argument that businesses think that they've got just about the right

level of security now, and that they can keep losses within boundaries and absorb them as a cost of business. If an ID check at POS didn't take any time and was 100 per cent reliable *and* didn't require new hardware investment *and* cost virtually nothing, then maybe they'd see it as useful. Otherwise?

In addition to this, businesses aren't likely to want to trust the accuracy, reliability and security of Government systems. The banks and credit card companies have run customer databases for years, generally fairly effectively and with relatively few security breaches. More recently the supermarkets have got fairly cute at running loyalty schemes, and while these can be vaguely sinister, they're voluntary, and there are limits to what the supermarkets can do with them without triggering massive PR disasters. Government, on the other hand, has shown itself incapable of getting absentee parents to pay for their children's upkeep, while Gordon Brown's own department is the one that gives away money on the Internet after massive ID theft from a Government department. Really, no sensible business that knows what it's doing as regards networks and personal data is going to want to play with these people unless the law forces it to.

Brown's team seems, rightly, to view identity management as a key issue for both the public and private sectors, but then confuses what the Government has been doing with what should be done, and what the private sector *will* do. "What [the Tories] are objecting to in the political sphere is going to be absolutely commonplace in the private sphere", says the source. That is, Brown still buys the notion that a centralised system with 'rock solid' ID based on biometrics is the way identity management is going to go, and that "as private companies acquire biometric security systems, their spread in daily life is inevitable."

The central fallacy here is that biometric systems provide 100 per cent verification of an individual, end of story. But they don't; the readers have major limitations, biometrics can be spoofed, and the more dependent we become on biometrics as an absolute 'guarantee' of ID, the more likely they are to be spoofed and subverted on an industrial scale. Microsoft UK CTO Jerry Fishenden had a lot to say about this earlier this year, and more recently produced a an illustrative fiction showing how in the near future widespread use of biometrics would lead to their subversion as an absolute 'gold standard' of ID. Nor do you always want 100 per cent rock solid ID that you can't subvert or override, as the cautionary tale of the finger shows.

The private sector, responding to commercial pressures and market requirements, *will* hone and refine its ID management systems (note that it already has these, and in the main they work), and it will to some extent introduce biometrics. But you won't see it introducing biometrics as 100 per cent across the board ID verification - more likely biometrics will be used to back up other forms of verification, or for highly restricted and policed forms of ID (i.e. if it isn't going to cost much and you can keep a lid on how many times it costs, maybe fingerprint is good enough). Nor will the private sector ID management systems produce

single centralised databases that form the key to everything there is to know about everybody in the country.

In the ID world according to Gordon, on the other hand, ID management will proceed down pretty much the path laid out by the architects of the ID scheme. It won't consider more decentralised and secure approaches that tailor levels of security to need, and although such matters will surely have to be considered by Brown's ID management task force (otherwise, what does it have to investigate?), Brown himself seems to be already pre-empting its report. Government ID management *will* however incur the vast levels of expense and complexity associated with the original ID scheme, and *will*, if Brown persists with the notion of expanding it to the private sector, collapse in even greater costs and complexities. ®

Biometric crack alert Careful readers may have noted the *Observer's* "Cars could be fingerprint-activated, making driving bans much harder to disobey." Something of this ilk might actually happen, as the police have already made noises (to the Transport Committee) favouring both this and remote disabling of vehicles, one of their beefs was that run-flat tyres were making stingers (the ones in the road, not the shoulder-launched missiles) less effective in stopping escaping vehicles. And there are also EU moves towards compulsory black boxes in vehicles. There are obvious problems and disadvantages associated with biometric activation of vehicles, but ask yourself why Gordon Brown thinks this has got anything to do with ID cards, and you get a pretty clear answer. The central idea is that it has *nothing* to do with the card and everything to do with the biometric that 'proves' absolutely that you're you. You're tagged for life, they always know where you are, what you can and can't do, who's looking for you and who you owe money to. Just thank the stars it doesn't work...

Dyning ID scheme alert: The *Sunday Times* reports that the Home Office has a more modest wheeze for making the ID scheme pay for itself. Charge every £8 every time they change their details on the NIR. This one's actually quite compelling as an idea - it would kill off the scheme far more swiftly and at less expense than Gordon's longer-ranging mega-disaster, and might just make John Reid even *less* likeable than he is already. We're impressed.