



Lockstep Consulting Pty Limited
11 Minnesota Ave
Five Dock NSW 2046

ACN 121 297 916

28 February 2007

Committee Secretary
Senate Finance and Public Administration Committee
Department of the Senate
PO Box 6100
Parliament House ACT 2600.

Dear Secretary,

Inquiry into Human Services (Enhanced Service Delivery) Bill 2007

Lockstep Consulting is pleased to make this submission to your committee's inquiry into the draft Access Card legislation.

Yours sincerely,

Stephen Wilson
Managing Director
By e-mail.

Summary

The Access Card plans do not yet embrace the full potential of smartcard technologies to enhance consumer privacy and online safety, probably because the project is "scoped in" under tight budget and timing pressures. There is an array of privacy enhancements that are compatible with the expected Access Card platform. These could be implemented right away – or if need be, retro-fitted later – but only if the legislation allows. Public confidence and take-up of the card depend on getting privacy right, up-front. A huge opportunity to fully utilise this most important infrastructure investment might be lost if the Access Card Bill prematurely freezes the design of the chip, cementing possible privacy compromises, or inhibiting future safety improvements.

In Australia's traditionally "technology neutral" e-commerce legislative regime, the draft Bill is paradoxical in the way it attempts to fix detailed specifications for the contents of the chip. As the draft stands, it will be inordinately difficult to improve the system in future, deploy new privacy enhancing measures, or even simply rectify flaws to do with the way data is stored in the chip. The risk of a need to change these specifications is heightened when detailed design is scheduled to come after the legislation is passed.



Lockstep offers the following recommendations:

- There is no need for the legislation to be so specific about the contents of the chip.
- There should be a new independent ombudsman or similar function to review and oversee all new Access Card applications so as to manage the risks of function creep without over-legislating the chip design.
- To prevent the Access Card number becoming a de facto electronic identifier for indexing backend systems, it would be better for as many participating agencies as possible to have their customer reference numbers accommodated in the chip (and not merely Medicare and DVA numbers as currently drafted).
- Given that significant welfare fraud is associated with manipulating or counterfeiting dependants' details, more work may be needed on how dependants will be recorded and managed in the chip.
- When it comes to legislating for the consumer-controlled area of the Access Card, we should anticipate beneficial third party services and intermediaries that will benefit consumers by enhancing smartcard-based information management.

Declaration of interests of Lockstep Consulting

Lockstep Consulting Pty Ltd was established in early 2004 by Stephen Wilson, a leading international authority on identity management and information security. Lockstep Consulting provides independent analysis and advice on security policy and strategy, authentication and privacy. Sister company Lockstep Technologies is developing smartcard and Public Key Infrastructure (PKI) based solutions to enhance privacy and combat web fraud.

Recent Lockstep Consulting clients include Medicare Australia, the Australian Government Information Management Office (AGIMO), the Australian Divisions of General Practice, the World Bank, the Singapore Government, and ASEAN. Stephen is active in several policy bodies including the Gatekeeper Policy Committee, Smartcards and Information Security Australia, and the APEC e-Security Task Group. He was a founding member of the National Electronic Authentication Council (NEAC), and the previous Federal Privacy Commissioner's PKI Reference Group.

Setting the scene: The potential of smartcards to enhance privacy and consumer safety

Lockstep Consulting has previously submitted to the Access Card Consumer and Privacy Taskforce that the full spectrum of smartcard capabilities has yet to be elaborated, and that the corresponding upside for privacy remains underdeveloped. Thus the privacy debate is dominated by largely unnecessary fears and uncertainty. We wrote to the Taskforce that:

Smartcards differ from magnetic stripe cards in more ways than mere memory size. Their in-built computer processing power, cryptographic functions and ability to work autonomously provide major opportunities for enhancing privacy, far beyond the rather obvious point that identity theft needs to be curtailed. To ensure that the Access Card

delivers maximum value to the public and to the government, Lockstep recommends that the following unique capabilities of smartcard technology be more fully factored into the policy formulation and system architecture:

- **Mutual Authentication:** smartcards should be the clearly preferred means for accessing sensitive services online, to protect consumers against phishing, pharming, web fraud and spam, as well as identity theft.
- **De-centralisation of data management:** fraudulent card use can generally be better detected by the card itself rather than by data mining all health & welfare transactions, resulting in better consumer privacy protection, less invasion into routine transactions, and better system performance.
- **Multiple identifiers:** smartcards can store and manage diverse consumer identifiers, to preserve their existing relationships with backend schemes and systems, and thus resist unnecessary data linkages.
- **Anonymity:** smartcards can encrypt identifiers to protect against eavesdropping, and to 'firewall' business conducted in different domains using the one card.¹

At present the Access Card's principle weapons against fraud are quite narrow, comprising the enrolment, identification and photographing of all card holders, and the innate resistance of the smartcard to counterfeiting and copying. Perhaps this focus is a function of tight time and budget constraints. Many of the broader privacy and anti-fraud benefits could be realised later by software upgrades to the card; the smartcard platform fortunately appears to allow for retrofits, but the legislation might not.

What do we need to know about smartcards in order to write good law?

To bring capabilities and consumer benefits to the fore, we need to know a little more about the technology than the simple points that in contrast to magnetic stripe cards, smartcards are relatively immune to skimming, and that they can hold much more data.

Smartcards are microcomputers embedded in plastic. They happen to have roughly the same powers as the personal computers of the mid 1970s. Unlike the passive magnetic stripe card, a smartcard can tell what's going on around it. It can check what type of terminal device is trying to communicate with it, and can refuse to 'talk to' any system it does not recognise. This is what makes certain smartcards effectively immune to card skimming, and makes lost cards safe against prying or copying.

More generally, smartcards being microcomputers can be programmed with a variety of sophisticated features. They can act as intelligent proxies for their owners, delivering such vital security and privacy benefits as:

- decentralising and unlinking customer identifiers, literally keeping them safe in peoples' wallets and away from central databases and call-centres
- encrypting identifiers to enhance consumer privacy

¹ Lockstep Consulting *Submission on Access Card Discussion Paper Number 1*, 25 July 2006; see http://www.accesscard.gov.au/discussion/1C6_lockstep.rtf.

- locking identifiers inside the chip so they cannot be copied or counterfeited
- running private off-line security checks inside the chip, to spot lost or stolen cards and to detect such fraud as prescription shopping, without having to aggregate and data-mine all innocent e-health transactions
- logging users onto secure websites, safeguarding them against counterfeit sites, a critical issue with self-service and patient-centric online health resources growing in popularity
- checking the veracity of electronic messages purportedly sent by government agencies to consumers, to protect them from the scourges of phishing and spam, which actually represent the most serious threats to privacy today.

Progressive responses to the problem of function creep

The draft Access Card Bill appears to embody at least two distinct ways of heading off function creep. Firstly and explicitly, it provides heavy penalties for government officers or commercial parties who use the card outside the purposes of the Act. Secondly and implicitly, the draft Bill prescribes in detail the data to be stored in the Access Card chip, such that future changes cannot be made by regulation but will require amendments in parliament.

These are blunt instruments for containing function creep. Freezing the design of the contents of the chip makes it inordinately difficult to improve the system's functionality and privacy in future, possibly denying consumers the sorts of protections envisaged above. Worse, freezing the design harms our ability to rectify mistakes, or to correct any omissions in the drafting of the Bill (some of which we have identified and discuss later in this submission). We note that the government in fact plans for the legislation to pass before tenders are signed, and thus well before detailed design is done.²

Lockstep submits that a more progressive and flexible suite of controls over function creep is required. We do not claim to have a simple answer to this complex problem. One element of a progressive approach might be to create an ombudsman or similar function specific to the Access Card that would review and oversee all new applications for the infrastructure. A strong oversight function could support a less prescriptive specification of the contents of the chip, better responsiveness to emerging demands on the Access Card system (including problem resolution), and continuous improvement.

Problems to do with identifiers

Section 34 of the draft Bill lists three specific existing identifiers that, where applicable, will be held in the Commonwealth's area of the chip: Medicare number, Reciprocal Health Care Card number, and DVA file number. All Access Cards will also have a

² See "Golden noose tied to cards", *The Australian*, 27 February 2007, page 28.

unique Access Card number. No other agency identifiers or reference numbers are mentioned in the draft.³

There has been a strong implication to date (if not an actual directive) that the Access Card should not change existing relationships that individuals have with human services agencies. For instance, the Minister in late 2006 said: “There will be no ‘Big Brother’. We will not be amalgamating the agency databases or creating a centralised database holding all your information in one place. We will keep your existing agency records with the relevant agency – where they are now”.⁴

To achieve these policy goals, one would expect that all of a cardholder’s agency reference numbers would be accommodated in the chip, not just Medicare Australia and DVA numbers.

If other agency numbers are not held in the chip, then there will likely be a trend towards using the Access Card number as a convenient means to interface with other agency systems. This will especially be the case when individuals with an Access Card register with another DHS agency for the first time. The draft Bill appears not to have any mechanisms to prevent the Access Card number becoming a de facto identifier for indexing steadily more backend systems.⁵

Dependants’ information

We understand that young dependants who do not have their own Access Card will be represented in some way in the Access Cards of their parents or guardians. Given that significant welfare fraud is associated with manipulating or counterfeiting dependants’ details, we would have expected more attention to be given to how dependants will be recorded in the chip and managed in respect of integrity, authenticity and change control.

Consumer controlled information

Section 33 of the draft Bill defines two “areas” of the chip: the Commonwealth’s and the cardholder’s. The draft goes into great detail as to the structure of the Commonwealth’s area and the penalties for inappropriately modifying it, but has nothing to say about the cardholder’s area. The concept of the consumer having dedicated to them for personal

³ Item 10 in Section 34 of the draft Bill says that if an individual holds a benefit card, then their chip will hold “information about that card as is determined by the Secretary”. This clause is written in the singular, and yet the definition of benefit card in Section 5 includes several different types and is open ended. Furthermore, ‘information about a card’ is ambiguous. The Bill’s description of benefit cards would be challenging to implement as drafted, because it is not clear precisely which information is to be held in the chip, nor how much information could be involved.

⁴ The Hon Joe Hockey, Minister for Human Services, Speech to National Press Club, Canberra, 8 November 2006.

⁵ Interestingly this is analogous to the potential problem of the Access Card Number printed on the face of the card becoming a de facto identifier for third party humans reading the card.

use a portion of the Access Card memory has (correctly in our view) become entrenched in the vision of the system, and the Consumer and Privacy Taskforce is now considering how best to manage it. But because the detailed concept and rules to go with it are still evolving, there must be a risk that the tender requirements already released to vendors for the build of the system will not adequately address consumer-controlled Access Card resources.

More work clearly needs to be done on regulating how the consumer-controlled area – which represents a scarce and valuable resource – is to be safeguarded and managed. Consumers need safeguards not only against unauthorised reading of their personal data but the writing of data as well, not least because it is possible that their precious memory could be filled up without their being aware of it.

It may be that the government will address the consumer-controlled area in future pieces of Access Card legislation. If so, we would like to take this opportunity to submit some considerations that would improve consumer safeguards, as follows:

- No information should ever be written to the consumer-controlled area of the chip without the express consent of the owner. Further, in accordance with the Correction Principle in privacy law, it is essential that consumers are provided the means to view and amend information in their chip.
- The sorts of smartcard resources that can be made available to consumers go beyond simple memory. The legislation should be informed by the nature of such sophisticated resources as:
 - user-elected controls over who (and what systems) can read their data
 - user-elected controls over who (and what) can write data into their area
 - “mutual authentication” of smartcard readers and of backend applications, so that the card will refuse to ‘talk to’ unrecognised systems⁶
 - system functions like encryption and digital signatures to help secure transactions undertaken with the card.
- In practice, consumers will actually not have much *direct* access to the contents of their chip. This may seem a semantic point but there are important subtleties that complicate the way smartcards and their owners interact. Any computerised memory – be it in a PC, an MP3 player, a cell phone or a smartcard – is usually accessed and manipulated via an editor of some sort, such as a word processor. Moreover, the contents of memory must always be “rendered” to make it intelligible, converting the “ones and zeros” into words, images or sounds.⁷

⁶ Mutual authentication is one of the many security layers that can be deployed around smartcard data. While the use of a PIN is well known to lay people, mutual authentication actually provides more subtle and more powerful ways of protecting consumers against unauthorised intrusions.

⁷ A corollary is that computer memory almost always includes additional control data such as formatting instructions that are never visible to users. For instance, there are major differences between the appearance of web pages through a browser and the XML code in which the pages

Therefore there is always some sort of software program that intermediates a user's desires for their memory and the way that memory is actually managed.⁸

- Furthermore, the modern trend for digital devices is for third party value-added services to help users manage their content. We imagine for instance that health & welfare portals will in future assist Access Card holders collate, review and update important information in their chips. A simple example would be a Medic Alert-type scheme where a trusted third party ensures the pedigree of clinical data in the chip, while engaging the consumer directly in the process of defining and maintaining it. In the longer term, networked patient-centric health management and evidence-based medicine, being so information intensive, can benefit enormously from smartcard technology, to improve the completeness, integrity and privacy of patient records, public health data and so on. There are a host of important policy considerations here, around privacy and implied consent, yet there are huge opportunities for good public policy outcomes. It would be wise for the Access Card legislation to account for these sorts of possibilities.

End.

are written. Therefore, Section 36 of the draft Bill is problematic when it states without qualification that "the Commonwealth's area of the chip ... must contain only the information specified in subsection 34(1)". It is inevitable that the chip will contain more information than specified in s34(1) – not just formatting but also cryptographic keys, 'master keys', authentication codes, certificates etc. – and that the precise nature of that information cannot be known until design is completed.

⁸ This reality means that legal ownership of the smartcard is only one factor that determines the consumer's ability to effectively control the data in their chip. Additional applications and services must come into play. We would stress that these points are not inherently negative but they do need to be considered by policy and law makers.