Parliament No:	14
Session No:	2
Volume No:	95
Sitting No:	159
Sitting Date:	6-3-2025
Section Name:	Ministerial Statements
Title:	Review into Public Disclosure of Full NRIC Numbers on Bizfile People Search
MPs Speaking:	Dr Tan Wu Meng (Jurong),The Senior Minister and Coordinating Minister for National Security (Mr Teo Chee Hean),Mr Yip Hon Weng (Yio Chu Kang),Assoc Prof Jamus Jerome Lim (Sengkang),Ms Sylvia Lim (Aljunied),Mr Speaker,Ms Tin Pei Ling (MacPherson),Mr Gerald Giam Yean Song (Aljunied),Ms Hazel Poa (Non-Constituency Member),Ms Jessica Tan Soon Neo (East Coast),Mr Pritam Singh (Aljunied),Mr Leong Mun Wai (Non-Constituency Member),Mr Liang Eng Hwa (Bukit Panjang),Ms Ng Ling Ling (Ang Mo Kio)

REVIEW INTO PUBLIC DISCLOSURE OF FULL NRIC NUMBERS ON BIZFILE PEOPLE SEARCH

(Statement by Senior Minister and Coordinating Minister for National Security)

Mr Speaker: Ministerial Statement. Senior Minister Teo Chee Hean.

10.32 am

The Senior Minister and Coordinating Minister for National Security (Mr Teo Chee Hean): With your permission, Mr Speaker, may I request the Clerks to distribute a handout to Members, which I will refer to during my Statement? Members may also access the handout through the MP@SGPARL App.

Mr Speaker: Please proceed. [*A handout was distributed to hon Members. Please refer to **Annex 1**.*]

Mr Teo Chee Hean: Thank you, Mr Speaker. Sir, on 9 December last year, the Accounting and Corporate Regulatory Authority (ACRA) launched its new Bizfile portal to replace its existing system. Like its predecessor, the new portal included a People Search function. This function allowed users to search for and select the individuals associated with registered business entities whose information they wished to access through the purchase of a People Profile. So, there is a People Search function and the People

Profile function. The People Search function is generally available to everyone, anyone. The People Profile function sits behind a paywall.

But unlike the old Bizfile portal, which showed partial National Registration Identity Card (NRIC) numbers in the People Search results, the new Bizfile portal displayed full NRIC numbers. This caused public anxiety about how easily full NRIC numbers could be searched for and accessed. Therefore, the People Search function was disabled on the night of 13 December 2024.

The Minister for Digital Development and Information, Mrs Josephine Teo, and the Second Minister for Finance, Ms Indranee Rajah, held a media conference on 19 December 2024, during which they apologised for the anxiety caused. They explained what had happened and the Government's intent to change the existing practice of using partial NRIC numbers. Ministers Josephine Teo and Indranee Rajah also made Ministerial Statements to this House on 8 January 2025 and responded to requests for clarifications from Members.

To thoroughly review the matter, the Prime Minister directed the Head of the Civil Service to set up a Panel to review the Government's policy on the responsible use of NRIC numbers where it pertained to the Bizfile portal; second, to determine what led to the Bizfile incident; and to identify learning points so that similar incidents do not recur.

The Panel also reviewed the design and implementation of the People Search function and the response to the incident by ACRA and the Ministry of Digital Development and Information (MDDI), from the time public concerns arose on 12 December 2024 until the People Search function was disabled on 13 December 2024.

The Panel submitted its report to me on 25 February 2025. I reviewed the report and reported to the Prime Minister that I had accepted its findings and recommendations. After studying the report carefully, the Prime Minister agreed with its findings, its assessment of the shortcomings and the learning points identified. He said that the Government would take the lessons to heart to improve its processes and strive to do better. He directed that the report be released to the public and for the matter to be deliberated in Parliament. ACRA and MDDI have also accepted the findings and released separate media statements on their follow-up actions.

Hon Members would have had the opportunity to study the report, which was made public on 3 March 2025.

Sir, before we turn to the Panel's findings, I will briefly summarise the issues regarding the use of full and partial NRIC numbers. This is set out on the first page of the handout, which is the Annex to the Panel's report. Minister Josephine Teo had addressed these issues in her Ministerial Statement on 8 January 2025 to this House. So, allow me to recap these issues briefly.

The NRIC number allows the individual to be referred to uniquely and definitively. It is important to definitively refer to an individual by using the full NRIC number when required by law and for other purposes, such as for medical procedures and business transactions.

However, the NRIC number had also become used by some organisations, not just to definitively refer to the individual, but also based just on the NRIC number, to carry out important and sensitive actions. The use of the NRIC number in this way is unsafe, because the person's NRIC number is likely to be already known to other persons or organisations.

Some organisations and people had also come to assume that the use of partial NRIC numbers means that the full NRIC number is thereby concealed and protected. Sir, with the availability of online algorithms, it is now easier and faster to work out full NRIC numbers from the partial NRIC numbers.

The use of partial NRIC numbers, therefore, neither meets the need to have a definitive way of referring uniquely to an individual, nor does it offer effective protection from the full NRIC number becoming known.

To address these issues, the former Smart Nation and Digital Government Office (SNDGO), now part of MDDI, commenced a policy review in 2022. The review determined that we should take steps to stop the incorrect use of NRIC numbers for authentication and also move organisations away from the use of partial NRIC numbers. This would allow NRIC numbers to be returned to their proper use as unique identifiers.

The Ministers overseeing SNDGO were responsible for deciding the policy direction on the use of NRIC numbers. The Ministers endorsed the policy intent of returning NRIC numbers to their proper use as unique identifiers and the broad implementation approach to do so.

The Permanent Secretaries of SNDGO, and subsequently MDDI, had overall responsibility for the implementation plans in accordance with the guidance from the Ministers. SNDGO, and subsequently MDDI, knew the transition would take time and planned for the public sector to take the lead on both: (a) stopping the use of NRIC numbers for authentication; and (b) moving away from the use of partial NRIC numbers. It also started developing plans for public education and private sector engagements on the proper use of NRIC numbers and the risks of using partial NRIC numbers.

So, with that background, I refer Members to the second page of the handout, which is on the timeline of key events. The full listing is in the table in the report. Briefly, the key facts are as follows.

SNDGO had planned for the public sector to move first in a phased approach. On 5 July 2024, MDDI issued a Circular Minute (CM) to public agencies to stop the use of NRIC numbers for authentication and to start moving away from the use of partial NRIC numbers. MDDI conducted a briefing on 16 July 2024 for agencies, including ACRA, on the CM, and answered their questions on it. The video recording of the briefing and MDDI's responses to agencies' Frequently Asked Questions (FAQs) were disseminated to agencies the next day. ACRA subsequently sought clarifications via email from MDDI on how the CM applied to the display of NRIC numbers in the search results of People Search in the new Bizfile portal.

However, communications between the two sides were not clear. ACRA misunderstood MDDI's instruction in the July 2024 CM for agencies to "immediately cease any planned use of masked NRIC numbers, for example, in new business processes or digital products". ACRA interpreted this as a requirement to "unmask" or disclose NRIC numbers in full in the People Search function on the new Bizfile portal.

However, MDDI had intended that agencies could continue to use partial NRIC numbers for their existing external-facing use cases, but were not to introduce new use cases of partial NRIC numbers. To MDDI, ACRA's Bizfile People Search function was considered an existing use case because it was a service that was already existing in the old portal.

MDDI had also assumed that when agencies stopped using partial NRIC numbers, they would consider if NRIC numbers even remained necessary for those use cases. This would be in line with existing requirements under the Government's Instruction Manual on Information Communications Technology and Smart Systems Management (IM8).

Based on ACRA's interpretation of the July 2024 CM, ACRA then instructed its IT vendor on 17 August 2024 to make the requisite system changes to display NRIC numbers in full in the People Search function on the new Bizfile portal, which was then launched on 9 December 2024.

Sir, I will now move on to the Panel's findings, which are summarised in the third page of the handout. The Panel found that a confluence of several shortcomings on the part of both MDDI and ACRA, and how they had interacted with each other on this issue, led to the incident.

First, the Panel found that MDDI should have been clearer in its policy communications in its July 2024 CM. MDDI and ACRA staff did not realise that ACRA had misunderstood how the July 2024 CM applied to the new Bizfile portal. Specifically, MDDI should have explained key terms and phrases in the CM more clearly.

Although MDDI did make efforts to brief agencies on the requirements of the July 2024 CM and disseminated the video recording of the briefing as well as the FAQs to them, the relevant documents were not appended to the CM. So, if one referred to the CM, one would not have seen the other clarifications arising from the session that MDDI had with the agencies.

Second, there were internal shortcomings within ACRA in sharing and acting on the information from MDDI on the July 2024 CM. The FAQs mentioned earlier were not properly disseminated within ACRA by the officers who had attended the briefing and the officers who had received the video and the email of what had happened. And this contributed to ACRA's continued misinterpretation of the July 2024 CM and resulted in them making decisions based on incomplete information. These FAQs would, for example, have alerted ACRA that stopping the use of partial NRIC numbers did not mean showing full NRIC numbers in every case, and agencies could decide to drop the use of NRIC numbers altogether.

Third, the Panel found that MDDI should have paid more attention to the implementation plan for new use cases of partial NRIC numbers that were more complex, such as public registries. The Panel found that, in directing agencies to stop new use cases of partial NRIC numbers, MDDI did not differentiate between simpler use cases, like one-to-one correspondence between public agencies and members of the public, and more complex use cases, like public registries, which could potentially disclose a large amount of data to third parties performing searches.

ACRA, as the national business registry of Singapore, is one such public registry. One of ACRA's functions is to provide public access to certain information in the registry, so as to maintain corporate transparency. The standard approach for public registries is to have safeguards, such as a paywall, so

that, as far as possible, access to the needed information from the registry is available only to users for whom the service is intended. But there is also often a search function for the registry, before these safeguards, which is open to everyone to narrow down the information in the registry which the user wishes to access, and agencies have to determine how much to reveal when someone performs a search without having to go through safeguards, such as a paywall, for the information. For such complex use cases, additional guidance from MDDI would have helped agencies decide whether disclosing full NRIC numbers was necessary, and if so, determine what safeguards should be put in place.

Fourth, in deciding to disclose full NRIC numbers in People Search, ACRA did not first assess the proper balance between sharing full NRIC numbers and ensuring that they were not too readily accessible on the People Search function. This contravened the Government's internal rules on data management, namely, IM8, which ACRA was required to comply with under the Public Sector (Governance) Act (or PSGA).

Sir, ACRA's frame of mind when interpreting the July 2024 CM was influenced by its discussions with MDDI five months earlier in February 2024. In February 2024, five months earlier, ACRA had planned a change to its People Profile – the part after the paywall – to only provide partial NRIC numbers instead of the full NRIC numbers, which it had all along been providing. At that time, SNDGO had advised ACRA on the wider move towards stopping public agencies from using partial NRIC numbers. So, this was in February. Bizfile users had also given feedback to ACRA that full NRIC numbers were needed for corporate transparency. So, in view of this feedback and ACRA's exchange with SNDGO, ACRA decided to continue providing the full NRIC numbers in the People Profile function instead of making its proposed changes to partial NRIC numbers. So, this is the People Profile function, which is after the paywall, and these were events and discussions in February, five months before the events that occurred.

So, this exchange with SNDGO in February gave ACRA the impression that the policy intent was to "unmask" all partial NRIC numbers, which was not the case. But that was ACRA's frame of mind when interpreting how the July 2024 CM should be applied to the People Search function in the new Bizfile portal, specifically whether to continue providing partial NRIC numbers or to change to providing full NRIC numbers instead to the part before the paywall.

Nonetheless, even if ACRA was under the mistaken impression that the July 2024 CM required them to disclose full NRIC numbers in People Search, ACRA ought to still have, as required by IM8, assessed the proper balance between the public interest in sharing full NRIC numbers, which was to promote corporate transparency, and the competing public interest in ensuring that full NRIC numbers were not too readily accessible.

The Panel found that the design of the People Search function of the new Bizfile portal made individuals' NRIC numbers too easily available to those who were improperly using the People Search function in a way that went beyond its intended purpose.

Fifth, the review found that certain security features for the People Search function were not adequately implemented for the new Bizfile portal. ACRA had required its IT vendor to implement various security features in the People Search function of the new Bizfile portal to protect against unintended uses by, for instance, limiting the extent of searches allowed.

However, certain security features were not adequately implemented when the new Bizfile portal was launched on 9 December 2024. After disabling the People Search function, ACRA requested that the Government Technology Agency of Singapore (GovTech) review the security features of the People Search function. So, this was after the fact, after the People Search function had already been launched.

The review found that some security features, including the CAPTCHA functionality, were not adequately implemented, allowing potential data retrieval using scripts from 9 to 13 December 2024.

These security issues were rectified by the vendor in the revised People Search function before it resumed service on 28 December 2024. ACRA is following up with the vendor and considering all its available options. Without prejudice to any such options, the Panel noted that ACRA remains ultimately accountable for the implementation of the People Search function, even though it had contracted this to its vendor.

The sixth and last finding of the Panel was that the incident management after public concerns on the Bizfile portal surfaced on 12 December 2024 should have been better. Upon receiving the public feedback, ACRA and MDDI should have ascertained more quickly the key facts of how the Bizfile incident happened and ACRA should have disabled the People Search function sooner. Doing so would have addressed public concerns in a more timely manner.

The public communications and response to public concerns should also have been better coordinated and clearer. And in hindsight, the Government should have made clear to the public at the outset that moving away from the use of partial NRIC numbers did not automatically mean using full NRIC numbers in every case or disclosing them on a large scale.

The Panel noted that the incident took place before MDDI had begun public education and engagement on the proper use of NRIC numbers as a unique identifier. If you recall, the implementation of this was in the public sector and the engagement of the private sector had not begun yet. So, this exacerbated public concerns when full NRIC numbers were easily searchable and accessible in the People Search function, since many members of the public would not have been familiar with the issues associated with the use of NRIC numbers. The Panel was of the view that it would have been better for MDDI to have embarked on public education and engagement earlier than what it had planned.

Mr Speaker, Sir, the details of the Panel's findings are in the report. Having reviewed it, I agree with the findings. I would like to thank the Panel for their thorough work on this matter. As I had stated earlier, ACRA and MDDI have both accepted the Panel's findings and are following up to address the issues identified, as set out in their respective media statements.

Beyond the agencies involved, this incident offers valuable and important lessons for the wider Public Service. To meet changing circumstances and new challenges, the Public Service will need to continually update its policies and practices. Some of these changes will not be straightforward. How we communicate and implement them will be critical. The Bizfile incident demonstrates that close coordination and careful attention to detail are required. Sometimes, it is a single issue, but at other times, it can be a confluence of factors that can lead to such incidents. The lessons that the Panel has identified

will be disseminated across the whole of the Public Service. Agencies are expected to take them on board and apply them to their work to avoid similar incidents from recurring.

Sir, beyond learning lessons, accountability is important as well. The political office holders overseeing ACRA as well as the Smart Nation work in MDDI have overall responsibility for the organisations under their charge. And this is regardless of whether they had specific or direct responsibility for the actions that led to the shortcomings that occurred. So, this distinction between an overall responsibility that political office holders have for the organisations under their charge and the specific or direct responsibility for the actions that led to the shortcomings that occurred.

Both Ministers Josephine Teo and Indranee Rajah have publicly accepted this overall responsibility and also apologised for what has happened.

At the Public Service level, the Permanent Secretaries of SNDGO, and subsequently MDDI, were responsible for implementing the policy. The Chief Executive of ACRA was responsible for the new Bizfile portal's design and implementation. While the Panel did not find any evidence of deliberate wrongdoing or wilful inaction by the ACRA and MDDI officers involved in this incident, the shortcomings identified, including ACRA's contravention of IM8, should have been avoided.

Mr Speaker, Sir, I should make clear that this review panel was not a disciplinary process. While the Panel's report serves as a reference, any disciplinary action, if warranted in relation to individual officers, will need to be conducted in accordance with the applicable frameworks and processes in the respective public agencies involved, and this is only proper.

The Public Service Division, MDDI and ACRA have taken into account the findings of the Panel and have thus reviewed the roles, responsibilities and actions of the relevant officers involved in the shortcomings highlighted in the report. These officers include those whose actions contributed directly to the shortcomings, as well as senior management who were responsible for providing oversight and guidance to the officers and are responsible for the proper functioning of their organisations.

The agencies have assessed that while there was no malicious or wilful wrongdoing by the officers, there were inadequacies in their judgement and actions, and appropriate measures are being taken against them. These measures range from counselling to retraining to reductions in performance grade, which will carry financial consequences, such as a reduction in their performance-based payments.

As for ACRA's contravention of IM8, PSGA does not prescribe financial penalties for public agencies that contravene IM8, and there is a good reason for that. The cost of any financial penalties would ultimately have to be borne by the public purse if we impose a financial penalty on a public agency. And therefore, such penalties would not be meaningful. Instead, as I have stated, the necessary actions will be taken against the officers responsible. The PSGA is designed with that in mind.

The Ministers overseeing ACRA as well as the Smart Nation work in MDDI had overall responsibility for the organisations under their charge and the Prime Minister will take into account this incident in his evaluation of the Ministers.

Mr Speaker, Sir, the Public Service holds its officers to a high standard of conduct and excellence. Singaporeans deserve and expect this. Given the range and complexity of public services, from time to time, mistakes will be made. If there is misconduct or malicious intent, we will deal with it severely and those involved will be punished. Where there had been no malicious or wilful wrongdoing, due consideration should be given to whether the officers had acted in good faith when we decide on what actions to take.

And most importantly, the lessons arising from the incident must be learnt and internalised, not only by the officers involved or their agencies, but by the Public Service as a whole, so that they are not repeated.

Mr Speaker, Sir, trust in the Public Service is essential. Maintaining that trust is, therefore, central to how we operate. When things go wrong, we are upfront with Singaporeans on where we have fallen short. We conduct thorough reviews and make improvements to our systems and processes to serve Singaporeans better while remaining fair to our officers.

Sir, this recent incident, while regrettable, demonstrates the Government's commitment to continuous improvement, to uphold the trust that Singaporeans have placed in the Government and the Public Service.

Sir, I will be happy to take any clarifications.

11.03 am

Mr Speaker: Order. We will now have clarifications on the Ministerial Statement. I can see that there are many Members wanting to seek clarifications. So, I would like to take this opportunity to remind Members that pursuant to Standing Order 23, Members may seek clarifications on the Ministerial Statement, but no debate should be allowed.

Members can seek clarifications by way of asking questions. If any preamble is required and if it takes too long, I will interject and ask you to get straight to asking your clarifications. So, I seek Members' understanding to keep your clarifications clear and concise. I will ask the same of the Senior Minister in his responses.

Mr Pritam Singh.

Mr Pritam Singh (Aljunied): Mr Speaker, I have three clarifications for the Senior Minister. The questions are follow-ups from my Parliamentary Question filed for the 7 January 2025 Sitting. [*Please refer to "Explanation and Impact of Policy Change on Full NRIC Number and Further Measures on Public Education and Protection of Sensitive Identifiable Information", Official Report, 7 January 2025, Vol 95, Issue 148, Oral Answers to Questions section.*]

The first pertains to the CM of 5 July and this is found at pages 20 and 21 of the report. It is not clear from the report whether ACRA provided a list of all existing communication and correspondence with members of the public that used masked NRIC numbers. Did ACRA send this list to MDDI? When did they send it and what was MDDI's response? This is vis-à-vis paragraph 9 of CM.

The second question is on ACRA's conversation with MDDI. It started in February 2024 and it concerned the People Profile function, not the People Search function. At page 15 of the report, it states that from 5 July – that was the point in time when the CM was distributed – to early August, ACRA had, "sought clarification from MDDI on how the July CM should apply to ACRA's new Bizfile portal," which was the one launched on 9 December.

It begs the question: what clarification was sought by ACRA and what was MDDI's response? In the report, I note at paragraph 48, it states that on 30 July, an ACRA officer, who had not gone for the MDDI briefing and did not see the FAQ document that MDDI had emailed; and this officer asked MDDI if ACRA needed to cater system enhancements to remove the masking of NRIC numbers in the People Search function. So, it would appear that the new Bizfile portal already was going to continue what the old Bizfile portal was providing to the public: masked NRIC numbers in the People Search function.

So, it would be helpful to understand what clarifications were sought, because at this point it seems like MDDI confirming to ACRA that it can continue to display masked NRIC numbers in the People Search function "for now", but that it should be prepared for eventual unmasking at a point when MDDI was going to issue future guidance. So, at that point, 30 July, it would seem everybody is ad idem on the way forward. So, this I think is the point which begs further questions – what went wrong after this point?

Once again, there is emphasis in the report on paragraph 7 of the CM and the confusion, and Senior Minister has explained how new business processes were misunderstood by ACRA. But paragraph 9, as I alluded to, makes it quite clear that ACRA, in this case, was supposed to provide MDDI a list of their existing correspondence with members of the public using masked NRIC numbers. So, that really is the subject of my question: when was that done?

The final question is, at what point did the senior leadership of ACRA fully reviewed the new Bizfile portal before it went public? Was there any independent assessment done about the full unmasking of NRIC numbers on the People Search function? I ask this question because in the conclusion of the report, it states that ACRA did not first assess the proper balance between sharing full NRIC numbers and ensuring that they were not too readily accessible. So, did they assess this balance at any point in time?

Mr Teo Chee Hean: Mr Speaker, first, I would like to thank Mr Pritam Singh for having read the report in such detail. That is very useful and he should also understand the conclusions that were arrived at in the report and what I had just said. In fact, he has identified all the misunderstandings in the communication between the two agencies which led to this unfortunate incident. In fact, this is described in the report as well as in my speech just now.

The two were communicating with each other but they had different frames of mind and therefore, they went away with different understandings of what the CM said and also different understandings of the communications and emails that they had with each other. In fact, that is really what was identified as one of the shortcomings in the report and in my Statement just now.

So, indeed that is the case. There was a gap in understanding between the two agencies. In spite of the fact that they had communicated with each other, each went away thinking that they had put their

point across clearly and each went away thinking that the other understood what was to be done and what was meant. But that was not the case.

Did ACRA send all the instances and so forth? I am sure they have, but the relevant point is that they were communicating on this particular instance and had a gap in understanding between the two.

Did ACRA make an assessment? They probably did, but as I pointed out, and as the Panel pointed out, they did not make a proper assessment of the balance between their function of making such a registry available and conveniently so to users, and the need to manage the access to information in such a search function. So, that was a shortcoming on the part of ACRA.

Mr Speaker: Ms Jessica Tan.

Ms Jessica Tan Soon Neo (East Coast): Mr Speaker, while the report did not indicate that there was any malicious intent or wilful action, the findings of the review panel did indicate that the Government's internal rules on data management policies were contravened, and Senior Minister Teo touched on the point of public trust.

As Government agencies store, access and handle personal information of Singaporeans in engagements and provision of various Government services and with digitisation, what assurances can be given to Singaporeans on the proper handling of personal data by Government agencies? Because it is not just about policies, it is not just about rules; it is about that balance.

I actually worry that it may come to the point of everyone being so afraid to move forward because of that. But it is a difficult challenge. Given this incident and the learning from this instance, it may lead to everyone being overly cautious. I need to understand what will be done across the Government to help our officers move forward and be able to make that right judgement call. It is not an easy problem to address.

Mr Teo Chee Hean: Mr Speaker, perhaps this is an opportunity to explain the process for ensuring data privacy and making sure that data is properly dealt with in the public sector versus the structure for the private sector.

In the private sector, there is the Personal Data Protection Act 2012 (or PDPA) and in the public sector there is the PSGA. And they largely mirror each other. In fact, some of the things that are in PDPA today, were originally already in the public sector's rules for data governance in IM8, even before PDPA was announced. And some of the things that were eventually enacted in PDPA and the guidance provided by the Personal Data Protection Commission (PDPC) were also adopted in the public sector. So, the two mirror each other.

But there are a couple of important differences between the two and I will take this opportunity to explain what they are.

First of all, there is no expectation within the private sector that different private sector corporations interact with one another and share data with one another, purportedly to serve the customer better. In fact, private sector agencies are quite protective of the data that they have because they see that as a

competitive advantage, and we also do not allow private sector organisations to sell their data to others for profit. So, by and large, they do not share with others.

In the public sector, there is an expectation that to serve citizens better, there is some sharing between the two. We sometimes hear, in Parliament also, "You already know this. Why do you keep on asking me for it?" So, in order to serve residents better, we do share data and this is allowed in the PSGA.

For example, you apply for a Housing and Development Board (HDB) flat, access your Central Provident Fund (CPF) account and all those kind of things, it is shared and available. If someone applies for social service support, that information is available so that the person in a distressed situation already does not have to keep on providing the same information again.

So, that is an expectation and it is different between the private sector and the public sector.

There is another important difference, which is what the financial penalties are. First of all, in the PDPA, the financial penalties are directed against the organisation; whereas in the PSGA, as I explained, if you direct the financial penalties against a Government agency, it is actually not very meaningful, because they all come, eventually, from the public purse. So, the financial penalties arise from actions taken against individual officers.

In the PDPA, originally, there were no specified penalties against individuals. Eventually, in 2020, the PDPA took some of the provisions in the PSGA and imported them into the PDPA, so that in some circumstances, the PDPA can be used to take action against individuals.

So, there is always a mirroring between the two and there are differences between the two.

First of all, the public sector does have a very strong and robust system for the management of data and the sharing of data, and for taking action against persons who contravene them. So, that is the start point.

Should this cause persons to become overly careful? I think that it is always a possibility whenever an incident such as this arises. But that is why it is important to identify the shortcomings clearly. Do not go in with a big bazooka and flatten everybody, but differentiate between the responsibilities of the individuals. Individuals who are responsible, they have to be held to account, but we must do so in a well-balanced and fair way to the individuals. This is the approach that we take and which we will continue to.

Mr Speaker: There are 14 hands that I counted. If the answer is already given by the Minister, please do not repeat the clarification. Mr Liang Eng Hwa.

Mr Liang Eng Hwa (Bukit Panjang): Sir, I refer to paragraph 48, which is about the exchanges between MDDI and ACRA. I read in that paragraph, where in the reply from MDDI to ACRA, it states that "ACRA can continue to display masked NRIC numbers in the People Search function for now". And it continues to say that it should be prepared for the "eventual unmasking of the NRIC number".

Can I ask the Senior Minister whether that remains the policy position – the eventual unmasking of the NRIC number? And in the case of the People Search function, what is the direction ahead? Would ACRA

eventually stop displaying the masked NRIC number? Would the full NRIC number be shown in some way, with some controls or with some safeguards?

My second clarification is related to page 16 for the chronology of key events. The report mentioned that ACRA did have internal deliberations about the risk of showing full NRIC numbers in the People Search function. It shows that ACRA did have concerns, at least, at the working level, but they went ahead because they misunderstood the instructions from the July 2024 CM. Can I ask if there is a deeper issue here, where an agency felt compelled to just go ahead with the launch even though internally, they have some serious concerns or reservations on the public implications? And whether does the Public Service have the mechanism where officers at the working level who may have spotted a potential high-risk situation, for example, in the upcoming implementation, are able to flag out these concerns and get attention from the management?

Mr Teo Chee Hean: If I may just say what has happened to the People Search function, the part before the paywall. ACRA has resumed service on that function, but without NRIC numbers, whether full or partial. Because they have done an assessment now and have come to the conclusion that it is possible to serve the intended users without having to use full or partial NRIC numbers, and that is what they have done. So, that is the situation.

Mr Liang has also read the report very, very carefully – and I am glad that he has done so – and identified certain places where there were gaps. Indeed, they communicated with each other and in the communication that Mr Liang cited, that showed how the two of them misunderstood each other – what is new, what is existing, there was a gap in understanding. Was the new Bizfile portal new? Or was it an existing use case? So, there was a gap there.

Also, what does stopping the use of partial NRIC numbers mean? Does it mean that where you had partial NRIC numbers before, you just go and use full NRIC numbers? So, there was a gap there in communication between the two agencies.

The question that Mr Liang asked is, is there a process for making sure that agencies can communicate and do this? In fact, they did. MDDI conducted a briefing, engaged the agencies, answered the questions and disseminated them the next day.

Within ACRA, there were some shortcomings. There was a shortcoming that was identified by the Panel where they did not fully communicate internally what the position was. And therefore, when ACRA and the senior management were making decisions on this, they were doing so without the benefit of the additional information that had come out of MDDI's briefings and interactions with the agencies. I think that describes how they had a difference of understanding.

But as Mr Liang indicated, there is a more important aspect here, which is that officers, especially at the senior level, need to understand the intent behind what the policy is – and certainly, officers at the senior level should be able to do so – and not implement things which are just going by the letter. And if there is a problem and there is an issue, they should engage with each other and thrash that out thoroughly. And I think that is one of the important lessons that we have learnt from this case.

Mr Speaker: Ms Sylvia Lim.

Ms Sylvia Lim (Aljunied): Thank you, Sir. I have two clarifications for the Senior Minister.

First, I found what he said about the overall accountability of Ministers very interesting. He mentioned that the two Ministers involved would have this incident taken into account by the Prime Minister in his assessment of their overall performance. But the fact is the Prime Minister is the Minister for Finance and ACRA is a Statutory Board within the Ministry of Finance. So, how does that work as far as the Prime Minister is concerned? Because he is also overall responsible for ACRA, in that sense.

The second clarification is about the report's shortcoming number six, which talks about shortcomings in incident management after the public concerns were raised on 12 December. I am personally aware that it is a reality in the Civil Service, and probably private sector, that in December, there are many staff that are on annual leave, we expect them to clear their leave. And December is usually a time when there are less staff around.

So, I would like to ask him whether this aspect of key decision-makers not being so readily available, did it feature at all in causing any delays in the incident response? And does he think that this could be a potential issue, even if it is not an issue in this case?

Mr Teo Chee Hean: The second point first, Mr Speaker. Certainly, it could have been a factor. But to the Panel which reviewed the thing, it was not an acceptable excuse or reason. The agencies still have to be responsible for what they are doing, whatever season of the year it is. So, that was not something which the Panel took into account – and I think rightly so.

On the point of the Prime Minister's responsibility, well, the Prime Minister is responsible for everything. But he has to delegate his responsibilities to Ministers who are responsible for Ministries, agencies and functions. That is part of the Prime Minister's role. If the Prime Minister tried to be responsible for everything, he would not be able to function at all. One of the responsibilities of the Prime Minister is to know when he should delegate and when he should intervene. I hope that Ms Sylvia Lim appreciates that.

I am also glad to note that Ms Sylvia Lim takes accountability, especially accountability of leaders of organisations, as something which is very serious, and which should be accepted when mistakes are made.

Mr Speaker: Ms Tin Pei Ling.

Ms Tin Pei Ling (MacPherson): Thank you, Mr Speaker. Three questions for the Senior Minister. First, on the incident management. I think there have been useful lessons drawn. In this case, it was shared in the report that the lessons will be disseminated to the broader Public Service. I would like to ask who may be coordinating this for this particular incident. Also, looking ahead, should there be similar incidents or other crisis-type of incidents happening, who will be coordinating the response and making sure that investigations and responses are being done in a timely manner?

Because in this case, I think there was a time gap at the beginning, so it allowed a lot of doubts and questions from the public to foment. With digitalisation, information and speculations got worse as a result of that; it did not quite help with that sense of public anxiety. So, I wanted to ask if there would be someone or some body to coordinate this going forward, arising from this incident.

Second is that I think quite clearly from the report as well as the questions to and fro so far, there has been no malicious intent, no deliberate wilful inaction or action. It was really everyone trying their best to do what they think is right. As Government business gets more complex, there are so many issues at hand. How do we strike the balance?

On the one hand, ensuring that discipline is taken for errors being done and continuing to strengthen public trust, but on the other hand, continuing to encourage public officers to take calculated risks when necessary so that innovations can still happen, so that things can still move forward, and not to always be worried about what ifs and do not do anything at all. I do not think that will serve us well as well. So, how do we balance that? Because from the report, I feel a bit worried – are we going to hammer them too much? Because that may not be sending the right signal to the broader Public Service as well.

Lastly, which pertains to a question that I had asked as a supplementary question during the previous Sitting. Given that there are still enterprises using the NRIC number as authentication, what is the progress of the Government's effort in getting them to rectify this? If this is not the right platform for me to ask this, I will file a question separately.

Mr Teo Chee Hean: I would like to thank Ms Tin. She has also read the report very thoroughly. I am glad to see that.

There is an existing process within the Government for actually coordinating across. And certainly, in the Public Service. There is the Committee of Permanent Secretaries, which meets regularly. They discuss issues of importance and issues where coordination between Ministries and agencies should take place.

But apart from that, although the digital world, as Ms Tin correctly points out, spins faster, we also use digital means very often in communicating with each other. I am sure that among the Permanent Secretaries, they will communicate with each other. They probably have their own address group, where things which are important, which have to be acted on quickly, are communicated with each other. In fact, because in this day and age, people also travel a lot, so wherever they are in the world, they will also know what is happening. It is a faster process as well in disseminating information and also making sure that things are understood.

I should say that by and large, the Public Service actually works very well and coordinates very well. Instances like this do take place, but they are, fortunately, few and far between. But they do take place. So, how do we deal with instances like this and the officers who have come short in their performance?

I think Ms Tin, and Ms Jessica Tan also, pointed out quite importantly, we should not come down like a tonne of bricks on officers for issues like this, even if they have become public and have caused public anxiety. We should deal with them fairly and in accordance with the Public Sector's disciplinary processes.

This is something which I think will give assurance to our officers that just because the thing has become publicly known and caused some anxiety, that we will come down on them in an unfair way. We have to evaluate what they did, what they did not do, what they should have done, what was the intent behind it and then decide on the appropriate action to be taken.

And that is the way that we should continue to deal with the Public Service so that our Public Service will continue to do all the things that they need to do for us, including taking calculated risks, if they need to, but not take risks dangerously.

So, these are things which we should continue to be able to do with our public officers.

On the enterprises' use of NRIC as authentication, the Public Service has stopped this practice within the Public Service. There is appropriate guidance going out to private sector organisations to also cease this practice because it is quite unsafe. This is something which is ongoing. If there are private sector organisations which do not realise that they should stop using NRICs for authentication, I think they probably have not been paying any attention to the media on this issue at all.

But I should explain what is the difference between authentication and using an identifier because there is still a little bit of confusion.

Let me give an example, say, email. All of us have an email address and quite often we even use our own name as the email address. We want the people whom we interact with to know our email address so that they can contact us. So, the email address is an identifier of one form and in fact, it is unique because the email service provider has to have the unique names, otherwise it will go to the wrong person. So, you actually make your email address available to others.

But for authentication purposes, it is quite different. You do not tell your password to others. That is something which you keep for yourself and your email service provider knows. So, there is a difference between an identifier and an authentication.

This is an example in which most people will understand that, yes, you can use your name as your email address. That is not insecure, and it is very often convenient and expected. But please do not use your name as your password or your NRIC as your password because, a good number of people know it. So, that is the difference between the two.

Mr Speaker: Dr Tan Wu Meng.

Dr Tan Wu Meng (Jurong): I thank the Senior Minister for the Ministerial Statement. I have asked two Parliamentary Questions on the same topic in January. My clarifications will fall into two buckets. The first on mindsets and instincts. The second on IT security.

Sir, firstly, on mindsets and instincts, can I ask, in hindsight, could there have been earlier involvement of agencies with a specific security mindset when the new Bizfile portal was being designed and implemented? In particular, does the Senior Minister agree that in the modern era, we must assume that any database with a search function will attract cyber troublemakers trying to download and scrap as much of the information as possible? And as such, how can we further strengthen the instincts or even the sixth sense within agencies and officers to be more sensitised to these dangers, especially for databases that contain NRICs, because the NRIC number is unique and cannot be changed? Once it is being harvested, that bell cannot be unrung.

Secondly, on IT security, can I ask the Senior Minister is there room to strengthen the red team capability and the use of red teams within the Government to look at the security of online portals that

might provide access to personal data even through a search function, especially for projects where there is a greater risk if there is a security glitch? For example, and I have read the report, it mentions that ACRA outsourced the portal security to the portal vendor. The vendor then outsourced security penetration tests to a security reviewer. And yet, when GovTech came in, they discovered that the security features were not adequately implemented. In this vein, do we know if the same portal vendor and the same security reviewer are providing services to any other Government portals or Government organisations?

Mr Teo Chee Hean: Sir, hindsight is a marvelous thing. I use it very often myself too. But in any situation, each organisation and each leader has to make the decision based on the information that he has and is able to obtain.

Specifically on IT security, yes, indeed, it is important that when organisations implement an IT system or change an IT system, that they take security into account. In fact, that is one of the requirements of IM8 and which organisations often find a little bit too prescriptive and overbearing. But that is a necessity and for the reasons that Dr Tan has pointed out. So, we do do that.

And I should say that the Government does not try to build every IT system itself. There are very reputable IT companies and vendors out there which the Government should make use of. And there are also very reputable IT security companies out there, some of them are at the leading edge of IT security, which the Government should also make use of. So, we should not and do not need to try to do everything ourselves. This is the approach that we take. And in the evaluation of whom to assign or whom to award the tenders to, these are taken into account.

But, of course, just as the Government can make mistakes sometimes, the IT vendors too, are not perfect, as we know. Even IT security companies or companies which sell IT security as their main product have made mistakes and been penetrated in an embarrassing way before. So, we need to keep on being vigilant.

I should say, without going into too many details, because we do not want to give away exactly what we do in maintaining IT security, we do have a system of red teaming, which is quite rigorous. And we also invite the public to help us. We actually have a bug bounty system, one which is evergreen. That means, if you do find a bug or you do find a way in which you can penetrate a Government system, you let us know, and there is a bounty for it. And this is evergreen.

But we also do, from time to time, have a hunting season. So, for certain of our systems, we invite white hatters to attack those systems. And then, we also have a bounty system for that. So, indeed, we have a system for that.

But for our process for choosing vendors, both IT vendors, as well as security vendors, I should say that if a vendor has been found to not have fulfilled his responsibilities properly, we take that into account in future awarding of tenders, because then, how can you be sure, as Dr Tan has pointed out.

And I am very careful with what I am saying, because as I pointed out, ACRA is keeping all its options open with regard to the IT vendor. But ultimately, the organisation which owns the system, which is ACRA, has ultimate responsibility for it. And ACRA accepts that responsibility.

Mr Speaker: Ms Hazel Poa.

Ms Hazel Poa (Non-Constituency Member): Speaker, I have three clarifications for the Senior Minister. Paragraphs 76 and 77 of the report tells us that the vendor was the one who appointed the independent security reviewer, not ACRA. And the report was not submitted to ACRA directly from the reviewer, but it was, in fact, the vendor who submitted the report on the test on its own product.

It appears to me as if this process has huge potential for abuse. Is there no concern over this procedure? Does it meet with the governance standards for the public sector? That is my first clarification.

My second clarification is: it is obvious from the report that ACRA did realise that there is a conflict between its understanding of the July CM with its obligations under IM8 and PSGA. Why did ACRA prioritise compliance with the July CM over compliance with IM8 and PSGA? And will there be instruction or guidelines given to organisations how they are to deal with such situations when they find them themselves in apparent positions of conflict? For example, it would appear from the report that ACRA sought clarification primarily over emails. Would it not be better to have a conversation or a meeting over this to sort out any misunderstandings? That is my second clarification.

My final clarification is: in paragraph 26 of the report, the Committee noted that we cannot just look at the incident itself but also go upstream. But think the Committee did not go upstream enough. We need to go back and look at the decision to restrict the collection and the use of full NRIC number, which actually led to the creation of masked NRIC numbers, which then created a false sense of security and led to NRICs being used as authenticators even in the public sector. So, have we reviewed that policy decision to find out what are the learning points and if so, what are they?

Mr Teo Chee Hean: Perhaps, the last point first. I would commend Annex A of the report to Ms Hazel Poa. And indeed, the issues and the problems of using full NRIC and partial NRIC numbers are explained there. That is why we want to shift and make sure that we do not use NRIC numbers as authenticators and with regard to partial NRIC numbers, we should move away from that.

As I said, there is an issue with that because it is not sufficient to identify a person or to definitively refer to a person when that need is there. And the belief that using partial NRIC numbers, you can be more relaxed with it, because it is a partial NRIC number, it is not a full NRIC number. But you cannot be more relaxed with that because, in fact, the full NRIC number is easily discoverable. So, these are problems and issues which arose over time.

I do not think it is because of the rules with regard to collection, use and disclosure of full NRIC numbers that led to this. It may have contributed to this. Those rules on the collection, use and disclosure of full NRIC numbers I think still make sense. That particular guidance also pointed to people using NRIC numbers for things like lucky draws and so on – it was quite unnecessary – and also whether or not you should collect and retain a person's NRIC card, not just his NRIC number. So, there was some guidance on that. I think those still remain relevant.

And it could have led to the practice of people using partial NRIC numbers. And that is also a practice which has serious downsides.

So, yes, I would commend Annex A to Ms Hazel Poa.

On the balance in ACRA, I would not say it is a conflict, but you have to strike the right balance between the functions that ACRA is meant to provide, which is to have a registry which promotes corporate transparency, and you have to balance that against how you protect personal data. And that is something which ACRA should have considered to strike the right balance. They did to some extent but, I think, the full appreciation was not there.

Is it better to have conversations? Yes, it is, but, you know, nowadays with digital ability to communicate with each other in email, you can do so quite quickly as well. Setting up a meeting can take more time. You can use all modalities. But I do not think that was the fundamental issue. The fundamental issue was they both went away thinking that they understood what that was all about, but they had a difference in interpretation that was not resolved, resulting in this incident.

So, I think I have answered all of Ms Poa's questions.

Mr Speaker: Mr Yip Hon Weng.

Mr Yip Hon Weng (Yio Chu Kang): Speaker, I thank the Senior Minister for his explanation.

Section 4 of the report highlighted that MDDI's July 2024 CM lacked clarity, leading to misunderstanding in implementation by ACRA. So, could Senior Minister elaborate on the steps taken to enhance clarity in future communications to prevent similar incidents?

And secondly, how do we strengthen the clearance and approval processes within the Ministry to prevent similar issues from happening in the future, especially of such a misunderstanding, especially when it pertains to issues across different agencies? I think this is quite important because, as we move forward, the issues that the Government is dealing with is going to be more complex and it involves much more agencies coming together to solve similar issues.

Mr Teo Chee Hean: I thank Mr Yip Hon Weng. Indeed, the issues that Government has to deal with have become more complex and particularly, in the digital age where things are moving so fast. So, things which were adequate two years ago for the digital age may not be adequate today, or you anticipate that they would not be adequate in a year or two.

Some of the security features that we had were adequate in the past but may not be adequate today and in the future, and we have to keep on evolving and changing; and therefore, when we make such changes, there is always a potential for misunderstanding between agencies. It is important to communicate and this is, indeed, one of the lessons that we have learnt here – to be aware of whether what you are saying is understood in the same way by the person who is receiving it; and the person who is receiving it, should be aware that what he has received may not be what the person who communicated it intended.

This is not just a function of the digital age or email or anything, I mean, we are all familiar with the old games that we play telephone or whatever it is, you pass the message and then by the time it reaches the 10th person, it is completely garbled. So, we are all familiar with that. It is not a function of the digital age. It is a function of making sure that we communicate with each other clearly.

In this case, there were two specific uses of terms which the two did not understand in the same way.

What was new? So, MDDI thought that the Bizfile portal, the search function was not a new use case whereas ACRA thought that, well, it is a new use case. Then, what do you do when you stop using partial? Or have I to stop using partial now? That depends on whether it was new or not new. And if I stop using partial NRIC numbers, what should I do with them? And MDDI said, the intent was, you do not have to unmask the full NRIC number in every case; whereas ACRA's leadership thought that that was the direction to go. So, there are gaps in understanding and we just have to keep on working at them.

Mr Speaker: Mr Gerald Giam.

Mr Gerald Giam Yean Song (Aljunied): Sir, moving forward, will the Public Service move towards less collection and use of NRIC numbers when they are not necessary? For example, will Members who submit appeals to the Government on behalf of their constituents still be expected to submit their full NRIC numbers even when there is clearly no need for it, for instance, an appeal to the Land Transport Authority to construct lifts on a pedestrian overhead bridge?

Second, over 500,000 queries were made on the Bizfile portals' People Search between 9 and 13 December 2024, and this is far exceeding the usual daily traffic of 2,000 to 3,000. Has MDDI been monitoring, including on the dark web, for the sale of NRIC numbers, potentially exfiltrated during this period? And if leaked NRIC numbers are found, will MDDI notify affected individuals and help them to mitigate risks, such as identity theft or fraud, for example, by offering affected individuals identity monitoring services, credit monitoring or fraud alerts to prevent misuse?

Mr Teo Chee Hean: Perhaps, I will address the second point first and also, Dr Tan Wu Meng alluded to that because he talked about the collection and use of data, especially NRIC numbers.

I should point out, if the Member read Annex A, that you must expect your NRIC number to be known to quite a few people. In fact, I can still remember the NRIC number of some of my classmates and my National Service (NS) colleagues, because we used it all the time. So, I can still remember them. And so, you must expect your NRIC number to be known to others. While it is private, you must expect that it is not secret. So, that is the status and how you should treat NRIC numbers.

So, I think the most important impact to assess on this case is what is the impact on the individual. In this case, when an individual incorporates a company, starts a business, he has to register with ACRA. And in his registration with ACRA, he knows that the details of himself and his company must be searchable and accessible for corporate transparency reasons. So, he knows that his NRIC number may be searchable and may be known to any number of people who want to find out about what his business associations are with various companies and what his associations with previous companies have been as well. And this is to promote corporate transparency. So, he knows that.

And so, the fact that his NRIC number has now become known is not in itself something which the individual should find unexpected or surprising. The important thing for the individual is that he must not use his NRIC number in an inappropriate way, such as using it as an authenticator or as a password. And if he does that, he is quite secure.

Mr Giam asked whether or not we have looked at the dark web and so on, whether people are selling NRIC numbers. Yes, we do. In fact, we monitor the dark web for a variety of things, including this, and we have not seen any sale of NRIC numbers as such.

On the question of collection and use of NRIC numbers, actually, in the communication with the Government agencies, I think it is important to know who you are communicating with. You are not communicating with an anonymous person. You are communicating with a person who is your resident, who has a specific concern and therefore, should be prepared to identify himself and so on. So, I think that is quite proper and quite legitimate, especially if the person is making a request or has an appeal to be made. I think that is quite proper and appropriate, and should continue.

Mr Speaker: Ms Ng Ling Ling.

Ms Ng Ling Ling (Ang Mo Kio): Thank you, Speaker. I have two clarifications for the Senior Minister, but I want to first thank the Panel for making such a thorough investigation in a relatively short time. I want to respect the two Ministers for taking the courage to assume responsibility and make public apologies very shortly after the incident broke. And I also want to empathise with the Public Service officers who have been involved. I can imagine the guilt and stress that they must have gone through on discovering the mistakes and making right the processes for a live portal and the lessons learned. I also want to appreciate Senior Minister Teo for explaining rather complex issues and investigations in a very simple way for us to understand.

My first question is, does Senior Minister Teo find that the Inter-Ministry Policy Coordination and Implementation in this case weak?

A follow-up question is that I have my IT-trained husband to thank for understanding the difference between an identifier and an authenticator in the use of NRIC number. But in my conversations with many people from my constituency who have discussed about this whole incident, it actually takes some time for people to understand the difference because there is technicality involved. And I am increasingly concerned about emerging issues in the related issues of personal data protection and privacy, cybersecurity and cybercrimes. The coordination, there needs to be — inter-Ministry and inter-agency coordination in the Government is emerging to be a difficult topic and a very technical one, and I take lessons from how we are dealing with climate change and sustainability.

Mr Speaker: Ms Ng, you may want to get to your clarifications.

Ms Ng Ling Ling: My clarification is that, for important issues, like climate change and also earlier, the ageing population, we have Senior Minister-level and Deputy Prime Minister-level coordination, whether this whole class of issues on PDPA, PSGA, cybersecurity, cybercrimes should coordination be taken at a more senior level, at Deputy Prime Minister or Senior Minister level?

Mr Teo Chee Hean: Well, first, I want to thank Ms Ng Ling Ling for her comments on our officers and also on the Ministers. I think they will appreciate your understanding and empathy with what they are going through right now. I have spoken to some of the officers myself and told them and assured them that if there is a shortcoming, we have to deal with it. And I have assured them that we will deal with it fairly.

On inter-Ministry coordination, there are a number of different levels. We do have inter-Ministry committees and coordination mechanisms. Sometimes we are accused of having too many, but we do have quite a few of these. These also have to operate at the appropriate level.

At the Senior Minister or Deputy Prime Minister level, they tend to deal more with policy and not implementation on a day-to-day or immediate basis, because if you try and do that kind of thing at the Senior Minister or Deputy Prime Minister level, you will end up not being successful.

It is the same answer as I gave with regard to the Prime Minister. I mean he is responsible for everything, but if you refer everything to him, he will become the bottleneck and nothing will get done and things will get delayed. So, similarly, with coordination at the Deputy Prime Minister or Senior Minister level. At that level, what we try and do is to make sure that we set up a system in which the relevant agencies work with each other properly.

So, you will see that for scams, we were not very well-coordinated initially, but we did have an inter-Ministerial committee helmed by the Ministry of Home Affairs' political office holders, which brought all the different agencies together, including the banks and the Monetary Authority of Singapore (MAS), and engaged the platform companies. And as Minister of State Sun Xueling has recounted, we actually have achieved a certain amount of success in getting the different agencies together at the implementation level.

And so, you have to get things done at the correct level; so now, we are able to actually swing into action much faster. In fact, I think it was The Economist which commended us on being able to do this where other countries have not.

But if you try to do that kind of coordination and day-to-day action at the Deputy Prime Minister or Senior Minister level, I think you will end up with a very, very major bottleneck and it will not work properly. So, you have to do it at the correct level and we do that for cybercrime, we do that for cybersecurity as well, and we have similar structures.

The Member had a question on identifier versus authenticator. In fact, that is one of the misunderstandings that we have, which has led to this issue, because people began to use their NRIC numbers as authenticators, thinking that it is secure and secret. And therefore, since they were using the NRIC number as an authenticator they came to believe that the NRIC number should be kept secret.

So, if you ask me for my NRIC number, I would not tell you. But actually, you have to tell the person, because that is the way in which you can be definitively referred to. Otherwise, how do you refer to yourself definitively? So, there was a contradiction in the individuals' minds as to what the NRIC number is. And when some organisations and people started to use the NRIC number as an authenticator, they began to say, "Well, then I should keep it secret". But that is not the original purpose of the NRIC number. The NRIC number is meant to refer to you definitively.

As I said, we used to use it all the time. I still remember the NRIC numbers of my classmates and my NS colleagues. So, that is the proper use of the NRIC and it should be sensitive, but you must assume that it is not secret.

Mr Speaker: Mr Leong Mun Wai, you were not here when Senior Minister Teo started his address and you would also not have heard my comments earlier. No mini speeches, please.

Mr Leong Mun Wai (Non-Constituency Member): Mr Speaker, Sir, I had heard your comments.

Mr Speaker: Yes, but when the Senior Minister was addressing the House, you were not in the Chamber, when we started.

Mr Leong Mun Wai: And I have read the report very thoroughly.

Mr Speaker: Alright, good. Go ahead.

Mr Leong Mun Wai: Mr Speaker, Sir, first of all, I thank the Senior Minister for his Statement and the Government for releasing the results of this investigation, so that we can understand the whole incident better.

Mr Speaker, Sir, I have a total of six clarifications to make. The report shows that this NRIC number incident is a communication disaster of the Government, both internally and externally. For such a major change in policy which pertains to —

Mr Speaker: Mr Leong, if you have six clarifications, by all means, ask all six. But if preambles are needed, you heard me earlier and you said you heard me, there is no need to make too much preamble. If the clarifications can be just asked, that will be appreciated and that is required. Thank you.

Mr Leong Mun Wai: In paragraph 40 of the report, it was stated that this July 2024 CM was also emailed to senior Public Service Leaders, including those with key responsibilities in IT and data matters within their agencies. Can I ask the Senior Minister whether any of these senior leaders have voiced concerns over the CM?

And when did the political office holders first get involved in the inter-agency response to the feedback and media queries on Bizfile?

Was there any direction provided by the political office holders over the inter-agency response and the decision to disable the People Search function in Bizfile?

To many Singaporeans, including myself, the new policy does not make sense in certain areas. I agree with the Government —

Mr Teo Chee Hean: Mr Speaker, can I ask him to identify the clarification which he is asking?

Mr Speaker: Yes, that would be helpful.

Mr Teo Chee Hean: I have counted three already.

Mr Speaker: Yes, I have also counted three. Yes.

Mr Teo Chee Hean: Thank you, Sir.

Mr Leong Mun Wai: And I have three more. To many Singaporeans, including myself, the new policy does not make sense in certain areas. I agree with the Government that NRIC numbers, full or masked, should not be used as authentication, and that must be impressed on Singaporeans. Next question, why is there a need to do away with the masked NRIC policy? Given that it is still an added security measure, as an identifier, and is already an established practice?

Next question, has the Government considered that this policy reversal could be very confusing for Singaporeans, especially those that are not digitally-literate?

Okay, my last question. Many Singaporeans have raised concerns over whether our full NRIC numbers have been so compromised that there is no need to mask them anymore. So, my last question is, can Senior Minister confirm, whether there is any evidence to show that our full NRIC numbers have been compromised on a large scale already?

Mr Teo Chee Hean: Sir, I will answer the last one first. It is the same question that Mr Giam had asked me and I think I have given the reply. No, we do not and have not seen anything, say, on the dark web, and so on.

And this idea that full NRIC numbers are compromised, I think it starts from the wrong basis, which I have tried very hard to explain. Which is that the fact that somebody knows your NRIC number, does not mean that it is compromised. Your NRIC number is supposed to be known by those people who need to know it and so you must expect that your NRIC number is known to quite a few others. And that is why it should not be used as an authenticator.

Which leads me to partially answer Mr Leong's question, which is that it is precisely because those who are not so digitally-savvy have this mistaken impression that they can use the NRIC number as an authenticator, that partial NRIC numbers provide security, that we have to do this, because if we do not, then they will go away with this mistaken belief and continue to do so.

And it is, in fact, not easy to communicate this. That is why we have to do this in a very careful process and in part, it is partially the reason why we have this misunderstanding and gap in communication, even within the Public Service.

So, indeed, it is complicated. But I think it is something which should be done, particularly to protect those who are not digitally-savvy, who go away with the idea that, "Yes, my NRIC number is secret. Therefore, I can use it as a password. And partial NRIC number is very good, because it hides my real NRIC number, which should be secret." So, we should move away from that, especially to protect those who are not digitally-savvy, because they may not fully appreciate the unsafe nature and the dangers of doing that.

Then, he asked when the political office holders got involved in the public communications on the Bizfile portal issue. They got involved, I think, almost as soon as it became apparent that there was public anxiety.

Next question about paragraph 40 and the email to senior officers, yes, the July 2024 CM was emailed to officers. Did the officers voice any concerns? Well, in the process of putting in new directives or new

circular memos, and so on, there is a process in which the agencies who put this out and who are responsible for that domain area, communicate with the agencies which may be impacted, implementing agencies and so on; and MDDI did do so. So, there was a process for that.

I think I have answered all of Mr Leong's questions.

Mr Speaker: Assoc Prof Jamus Lim.

Assoc Prof Jamus Jerome Lim (Sengkang): Thank you, Sir. Could I just quickly confirm that it is the official position of the Government that it will, going forward, be actively working to discourage or dissuade the private sector's use of NRIC numbers in all authentication use cases, including the protection of confidential, but not necessarily secret information, such as, for example, health reports or bank statements?

I say this fully appreciating the distinction between identification and authentication, but nevertheless, caution against going overboard in pursuing best practice security. Because after all, it is not complicated for IT personnel to happily code up password hashes, but the consequences for the rest of us could be a much diminished user experience – needing to cross reference one-time passwords each time we wish to do something simple like retrieving our bank statement.

Mr Teo Chee Hean: Could I make a clarification that Assoc Prof Jamus Lim is suggesting that the Public Service should not adopt best practice security processes?

Assoc Prof Jamus Jerome Lim: No, I am asking, with regard to how the Government will now recommend private sector action. So, in terms of how it will dissuade the private sector from using these kinds of authentication method.

Mr Teo Chee Hean: I think Assoc Prof Lim did not answer my question. I thought I heard him say that we should not be adopting best practices. I want to confirm whether he thinks we should be adopting best practices or not.

Assoc Prof Jamus Jerome Lim: Of course, we should be adopting best practices. Let me be clear about that, yes.

Mr Teo Chee Hean: I thank Assoc Prof Jamus Lim for his clarification, because if he starts from a different start point that I start from, then we will be having quite a different set of answers to his questions.

I think the Government does want the private sector to adopt best practices in authentication. And I am glad that Assoc Prof Jamus Lim agrees with that. That is an important start point.

And the idea that you can use your NRIC as your password is unsafe, and we want to discourage that and we hope that the private sector will stop that; we will see how we can reinforce that in a much clearer way for the private sector.

Mr Speaker: One final clarification. Mr Leong.

Mr Leong Mun Wai: Thank you, Speaker. I got one final clarification for the Senior Minister. I still want to ask whether it is a better communication strategy and also maybe a better strategy in getting Singaporeans to not use their NRIC number, whether full or masked, for authentication, by just educating them on not using it for authentication. Rather than introducing one more factor, and say that, "Oh, we should discontinue the masked NRIC also". Because there are some advantages to the use of the masked NRIC.

Mr Speaker: Mr Leong, what is your clarification?

Mr Leong Mun Wai: Sir, I am asking, is it a better communication strategy and also implementation strategy, by just concentrating on telling Singaporeans that, "Do not use your NRIC for authentication", and not to confuse them with, "We are now not using the masked NRIC also"? You get what I mean? Because now you are introducing two things.

Mr Speaker: I think, Mr Leong, yes, you have asked your clarification.

Mr Teo Chee Hean: Sir, well, first of all, I take it that Mr Leong has no disagreement on what I have described as the dangers of using full NRIC as authentication. And I hope that in his ability to communicate with the public that he will also stress that. And that is an important message which all of us should take to the public, including Mr Leong.

But I also hope that he has read the Annex A and listened to my explanations as to why the use of partial NRIC numbers, in the belief that they provide adequate definitive identification, or that they are safe because it protects your NRIC number, which people mistakenly believe that it should be secret and cannot be revealed to anybody, that this is also the wrong belief.

So, I understand that the second part is indeed more difficult to explain. So, in the implementation, when we do this communication, I think I do agree with him – the more urgent and important thing is to tell people, "Do not use your NRIC number for authentication or as your password". I think that is the most important thing.

And then, we will have to shift people away from the idea that if you use the partial NRIC number, it is enough to identify you. It is not, uniquely. And the idea that if you use your partial NRIC number, it somehow keeps your NRIC number "secret", which is not so. So, that part, I think it will have to be a follow-up on the first part.

Sir, if there are no more clarifications, may I seek your permission just to make some remarks to round up?

Mr Speaker: Go ahead.

12.14 pm

Mr Teo Chee Hean: Mr Speaker, I thank Members for seeking clarifications and the many useful points that they have made.

The Government has conducted a thorough review over two months on what had happened, why they happened and how we can improve. A report has been released publicly and has been thoroughly discussed today in this House. I thank Members for seeking these clarifications because it helps to communicate to the public also why we are doing what we are doing.

Sir, taking reference from the shortcomings identified by the Panel, the Public Service Division, MDDI and ACRA have followed up to review the actions and responsibilities of the officers involved in relation to the Bizfile incident – and this includes both senior officers and leaders of organisations, as well as officers who are directly responsible. But as I said, and I thank Members for their support, that we will deal with them fairly.

The lessons learned that the Panel has identified are also being disseminated across the whole of the Public Service, so that agencies can take these on board and ensure that similar incidents do not recur.

Mr Speaker, Sir, even though the process and findings of the review may cause the Government discomfort and even some embarrassment, we have gone about this openly and transparently, and I am glad that Members on both sides of this House agree with that. This is so that the Government can account to the public and demonstrate its commitment to rectify shortcomings and serve the people better.

This has been and will continue to be the Government's approach when mistakes are made or shortcomings are identified from time to time. It is an approach which this Government is determined to continue, and it is a key pillar of good governance and for the good of Singapore and our people. [*Applause*.]

12.17 pm

Mr Speaker: Order. We have completed the Ministerial Statement. We will now go back into the Committee of Supply to debate the Estimates.

I have revised the commencement time of the Committee of Supply to start immediately. With the change in commencement time, the revised guillotine time for Head V, Ministry of Trade and Industry, is 2.25 pm. Hon Members will be notified of the revised conclusion times for the subsequent Heads of Expenditure.

The Clerk will now read the Order of the day.
