Parliament No:	14
Session No:	2
Volume No:	95
Sitting No:	149
Sitting Date:	8-1-2025
Section Name:	Ministerial Statements
Title:	Responsible Use of NRIC Numbers
MPs Speaking:	The Minister for Digital Development and Information (Mrs Josephine Teo),Mr Speaker,Mrs Josephine Teo

RESPONSIBLE USE OF NRIC NUMBERS

(Statement by Minister for Digital Development and Information)

12.29 pm

The Minister for Digital Development and Information (Mrs Josephine Teo): Mr Speaker, Members have filed a total of 51 Parliamentary Questions (PQs) on the National Registration Identity Card (NRIC) policy and the disclosure of NRIC numbers on the Accounting and Corporate Regulatory Authority's (ACRA's) Bizfile portal. Second Minister for Finance Ms Indranee Rajah and I will be making Ministerial Statements to address the issues raised. Our Statements will address Question Nos 1 to 37 for oral answer in yesterday’s Order Paper; Question Nos 3 to 8 and 39 to 44 for written answer in yesterday’s Order Paper; Question No 52 for oral answer in today’s Order Paper, and related questions that have been filed for subsequent Sittings.

Mr Speaker: Please go ahead.

Mrs Josephine Teo: Sir, let me start by acknowledging the concerns raised by the public over NRIC policy. The Bizfile incident is unfortunate.

Without intending to, it may have led the public to believe that the Government is changing its policy to allow full NRIC numbers to be exposed on a wide scale. This is not the case. We take the public's concerns very seriously and are very sorry that the mistake has caused them much anxiety.

I want to reassure the public that NRIC numbers remain personal data. NRIC numbers can only be collected when there is a need to do so. Organisations that collect NRIC numbers also have a duty of care. Subject to applicable law, they must notify and seek consent on use, and ensure protection of the data. These are existing guidelines that will not change.

However, there are also some incorrect uses of the NRIC number today. Our plan was to stop these incorrect uses while the problem is relatively contained. Doing so will better protect everyone and allow us to use NRIC numbers with confidence.

In this regard, my Statement today will address two issues: the current incorrect uses of NRIC numbers and why we need to change; and what our next steps will be.

Sir, when we interact with others daily, we are identified by our names. However, our names may not be unique. For organisations that deal with many people, say, a hospital with several patients named John Tan, they need a better way to uniquely identify them. Their NRIC number is a useful unique identifier in such situations. When the hospital needs to perform an operation or dispense medication, the doctor or nurse must make absolutely sure that it is the right John Tan they are dealing with and they should ask you, "What is your NRIC number?"

Since the NRIC number's purpose is to be a unique identifier, it cannot be a secret, just as our names are not secret. I should emphasise, however, that while your NRIC number is not a secret, it is not meant to be widely disclosed. This is the concern echoed in Mr Lim Biow Chuan's question.

We would only disclose our NRIC number under certain circumstances, for example, when required by law. Some examples include disclosing our NRIC number to our employers, at the clinic or when we subscribe to a mobile telephone line. Because we do have to disclose our NRIC number to others for such purposes, we must assume that at least some people know our NRIC number.

Over time, however, NRIC numbers have become increasingly used as more than an identifier. Previously, organisations would require seeing my physical NRIC card to confirm that I am who I claimed to be. However, some organisations assume that if someone can cite my NRIC number, that person must be me! This is clearly wrong.

On the assumption that this person is indeed me, some organisations may go further to give the person access to privileged information or services. When used this way, my NRIC number is no longer just an ID, or identifier, but a key to unlock more information or services. In such situations, the NRIC number is being accepted as an authenticator, or proof of who a person claims to be. This is clearly inappropriate.

Instead of the full NRIC number, some organisations collect and use a partial NRIC number, usually the last four characters of the NRIC number. They think that this is safe and that revealing only the last four characters still keeps the full NRIC number secret. Among public agencies, even when the agencies had the full NRIC numbers, the use of masked NRIC numbers became more common.

Besides organisations, some individuals also started to use their NRIC numbers as their passwords. They did so under the impression that the full NRIC number is secret.

However, as shown by Dr Tan Wu Meng in his question, there are now algorithms that can be found online, that have made it easier to work out the full NRIC number from the partial or masked NRIC number. The easy availability of such algorithms means that the continued use of partial or masked NRIC numbers gives both organisations and individuals a false sense of security. This does not really keep the

full NRIC number secret. This also makes the practice of using NRIC numbers as passwords even more inappropriate.

To the questions by Dr Tan, Mr Liang Eng Hwa and Ms Sylvia Lim, these developments led the Government to take steps to stop the incorrect uses of the NRIC number. This meant two things: one, not using the NRIC number as an authenticator; and two, moving away from the use of masked NRIC numbers, because it creates a false sense of security.

We knew this transition would take time. But it was better to start while the problem is relatively contained and for the Government to take the lead.

To the question by Ms Joan Pereira, we proceeded to ask agencies to stop using the NRIC number as an authenticator or as a password. We also asked agencies not to plan new uses, with a view to discontinuing existing uses of masked NRIC numbers eventually.

The lapse in coordination between agencies led to ACRA's misunderstanding and the disclosure of full NRIC numbers in the People Search function of its new Bizfile portal.

In hindsight, what we should have made clear was that moving away from the use of masked NRIC numbers did not mean automatically using the full NRIC number instead, in every case. At no point was our intention to disclose full NRIC numbers on a wide scale.

In place of masked NRIC numbers, in some instances, there would be no need for the NRIC number at all. In other instances, names alone or some other identifier would be sufficient. But there could also be instances where full NRIC numbers should be used, instead of masked NRIC numbers. Each case would have to be assessed and decided individually.

Members including Mr Leong Mun Wai, Mr Liang Eng Hwa, Mr Xie Yao Quan, Ms Jessica Tan, Mr Dennis Tan and Mr Pritam Singh have asked about the internal processes leading to ACRA's actions. Minister Indranee will say more about it in her Statement later and address Members' questions related to ACRA.

Miss Cheryl Chan asked why the efforts to change did not include the private sector. The Government knew that it would take time for public agencies to make the change. We expected that it would take even longer for the private sector because of long-standing practices and habits. The plan was therefore to change the internal practices of Government before moving to change practices in the private sector and non-profit organisations, which Ms Usha Chandradas asked about. We believed that doing so would allow us to better understand the implementation challenges and, as a result, facilitate a smoother transition in the private sector.

We had also planned to mount a major effort to help Singaporeans be aware of the risks and to support efforts to stop incorrect practices. The Bizfile incident was an unfortunate misstep which now means these plans need to be brought forward.

While we had taken steps to stop the incorrect uses of NRIC numbers in the public sector, we had not started implementation for the private sector. Mr Edward Chia, Mr Liang Eng Hwa, Ms Hazel Poa and Mr Xie Yao Quan have asked specifically what should be done in the private sector.

At this stage, we would advise private sector organisations to do two things: first, private sector organisations that are using NRIC numbers as a factor of authentication or as default passwords should stop this practice as soon as possible; and second, private sector organisations that presently collect partial NRIC numbers to identify people can continue to do so. The guidelines for the private sector have not yet changed and we will only consider how they should be updated after consulting the public.

To questions by Mr Xie Yao Quan, Mr Melvin Yong and Mr Sharael Taha, we aim to start consultations soon and will provide details when ready. Our initial soundings with the private sector suggest there can be different approaches. Some organisations currently using partial NRIC numbers can stop the practice and replace them with alternative means of identification such as mobile numbers or email addresses or drop them entirely. But there are also organisations that need to accurately identify persons and can justify the collection of full NRIC numbers even if they are not required by law. For example, preschool centres will prefer to collect the full NRIC numbers of visitors rather than just the mobile numbers; the parents will certainly feel more secure. In applications for and disbursements of substantial financial aid, persons would also need to be accurately identified.

We will take these considerations on board when updating the guidelines. In any case, I would like to assure Members like Ms Jean See and Mr Ong Hua Han that the Personal Data Protection Commission will support businesses in changing their authentication methods. This will include raising their awareness on why the use of NRIC numbers as a factor of authentication is unsafe and working through the Infocomm Media Development Authority and the Cyber Security Agency's programmes to help businesses review and adjust their practices.

To questions by Ms Tin Pei Ling, Mr Zhulkarnain Abdul Rahim and Assoc Prof Jamus Lim, I should emphasise that NRIC numbers are personal data. This means that organisations collecting and using NRIC numbers must continue to exercise a duty of care. Subject to applicable law, they must notify and seek consent on use, and also ensure the data is sufficiently protected. Certainly, they should not disclose the NRIC numbers unless there is good reason to do so.

Members may also ask, if the NRIC number is not suitable as an authenticator, what about the physical NRIC card, our pink identity card? If we look at our physical NRIC card, we will see that it contains other identifying information, such as our photo and fingerprint. It allows others to check that the information on the card matches me, the person holding the card. In addition, the physical NRIC card is not easily faked. The physical NRIC card is, therefore, suitable as an authenticator, or proof of who I claim to be. But someone providing my NRIC number and claiming to be me, does not have these additional factors of proof.

Organisations must know that the physical NRIC card and NRIC number are different. The physical NRIC card can be an authenticator, but the NRIC number should not be used as an authenticator. Organisations should, therefore, not accept my NRIC number alone as proof that the person citing it is indeed me.

Besides organisations, individuals, too, have questions about what they should do. There are also two things. The first is to clarify their understanding of the NRIC number. Members like Ms Sylvia Lim asked about this.

We have said that our NRIC number is like our name. Even if it is not widely disclosed, it is not secret. In our daily lives, if someone we do not recognise calls out our name and starts to behave as though they know us well, we would be slightly suspicious. We might be polite but not too friendly. Certainly, we should not fully trust this person, just because they know our name.

This should also be how we treat anyone who tells us our NRIC number. We should not automatically assume that they know us well or are figures of authority or can be trusted. We should be cautious about revealing more about ourselves, or saying yes to their requests or following their instructions without checking further.

The second thing we can do as individuals is to review our passwords. If we have used our NRIC number as a password to access any information or service, we have mistakenly used it as an authenticator and should change the password immediately. Doing so will give us better protection against people who use our NRIC number to get access to information or services. It will also complement efforts by organisations to stop using the NRIC number as a factor of authentication.

To Ms Hany Soh's question, NRIC-related scams are not new. Most NRIC-related scams involve victims who think they are speaking to figures of authority and end up taking actions that harmed themselves, such as transferring money without further checks. Very few cases have involved scammers directly using NRIC numbers to unlock access to valuables.

Several Members have also asked how to mitigate the risks when NRIC numbers are disclosed. They include Mr Zhulkarnain Abdul Rahim, Mr Edward Chia, Mr Christopher de Souza, Mr Ong Hua Han, Mr Liang Eng Hwa, Ms Jessica Tan, Mr Louis Chua, Miss Cheryl Chan, Mr Sharael Taha and Mr Yip Hon Weng.

As I have explained, the risks arise from the incorrect use of the NRIC numbers. If individuals stop using NRIC numbers as passwords and organisations stop using NRIC numbers as authenticators, this will go a long way to preventing harms from scams and identity theft. They will give us all better peace of mind to use the NRIC number whenever it is necessary, such as to get medical treatment or apply for jobs.

Sir, the Government appreciates that the incorrect uses of the NRIC number may not be well understood. Our public education efforts will raise awareness among organisations and individuals, and to guide them on what they should do. In doing so, we will focus on the points I highlighted above.

Mr Gerald Giam asked about alternatives to the current NRIC number system. In fact, the risks do not arise directly from the structure of the NRIC number. Rather, the risks arise when the NRIC number, which is meant to be a unique identifier, is incorrectly used as an authenticator or a password. Even if we were to create an alternative identifier, we would still have a problem if organisations used it as an authenticator and individuals used it as a password.

Sir, let me turn now to questions about ACRA's exemption from Personal Data Protection Act (PDPA) requirements and the Government's data protection measures. These were raised by Ms Tin Pei Ling, Ms Sylvia Lim, Mr Saktiandi Supaat and Mr Patrick Tay.

The Government has always taken seriously its responsibility to protect the data entrusted to the public sector. The Government's personal data protection standards are set collectively by the Public Sector (Governance) Act, or PSGA, and our own internal rules.

The PSGA is aligned with the PDPA and adapted to the Public Service context. Our internal rules are comprehensive and take reference from international and industry standards. We also continually strengthen our data governance practices.

ACRA is expected to comply with these rules and the PSGA, which are no less stringent than PDPA requirements. Regular, mandatory audits are conducted to ensure that public agencies, including ACRA, comply with the standards for data protection and the security of information and communications technology systems. The number of data incidents and their severity is published annually.

In the most recent whole-of-Government audit exercise on information technology-related data security controls, there were very few significant findings and all of them had been remediated by the agencies concerned. There has also been a reduction in data incidents of medium severity and above. Where necessary, we have also taken public servants to task, for example, in serious cases involving unauthorised disclosure or improper use of information.

Members can be reassured that we take these rules and controls very seriously. We will continue to regularly review the safeguards to ensure that they remain relevant.

Sir, let me conclude. We understand the public's concerns about NRIC numbers. It was not our intention to make the full NRIC number widely disclosed and we are not heading in that direction.

NRIC numbers are personal data and can be collected and used only when there is a need to. Organisations that hold your NRIC number also have a duty of care. Subject to law, they must notify and seek consent on use, and ensure protections. These are existing guidelines that will not change.

What needs to change are the incorrect uses of the NRIC number. These include using NRIC numbers for authentication or as passwords. It is better to make these changes while the problem is relatively contained. Organisations and individuals can both help by taking steps to stop using NRIC numbers as authenticators or passwords.

By taking action as soon as possible, we can increase protection for all of us. This will allow us to more confidently use the full NRIC number as a unique identifier whenever we need to do so. Mr Speaker, please allow me to summarise a few key points in Mandarin, please.

(*In Mandarin*)*:* [*Please refer to* ***Vernacular Speech***.] Mr Speaker, the Government understands the public's concerns about the correct use of NRIC numbers. I would like to reiterate here that it is not our intention for the full NRIC numbers to become widely disclosed information.

NRIC numbers are personal data, and they can only be used and disclosed when there is a need to do so.

Unless indicated by law, organisations that wish to collect and hold your NRIC number must first notify and seek consent on its use, and ensure that it receives adequate protection. These existing guidelines

will not change.

However, what needs to change are some incorrect uses of the NRIC number. For example, we should not use NRIC numbers for authentication or as passwords.

It is better to make these changes and rectify the problem while it is still relatively contained. Both organisations and individuals can do their part to stop using NRIC numbers as authenticators or passwords.

By taking action as soon as possible, we can increase protection for all of us. This will allow us to more confidently use the NRIC number as a unique identifier, whenever we need to do so.

(*In English*): Mr Speaker, with your permission, I will respond to any clarifications which Members may have, after Minister Indranee Rajah has also made her Statement.

12.57 pm

Mr Speaker: The Second Minister for Finance will indeed also be making a related Ministerial Statement. I will allow Members to raise points of clarifications on both Statements after Minister Indranee's Statement. Second Minister for Finance.
