Office of the Clerk of the House of Representatives

Te Tari o te Manahautū o te Whare Māngai

15 October 2013

Hon Christopher Finlayson QC
Chairperson
Privileges Committee

Dear Mr Finlayson

Privileges Committee inquiry into a question of privilege regarding the use of intrusive powers within the parliamentary precinct

Thank you for your letter of 20 September 2013 inviting me to make a submission on several issues that the Privileges Committee is currently considering as part of its inquiry into the use of intrusive powers within the parliamentary precinct. I welcome the opportunity to make this supplementary submission. As I mentioned in my earlier submission on this inquiry, I am happy to assist further when the committee looks at setting guidelines for the disclosure of information from parliamentary information and security systems.

I have set out in the appendix to this letter my responses to the specific issues raised by the committee. In summary, my view is that the parliamentary agencies (the Office of the Clerk and the Parliamentary Service) would benefit from having clear guidelines as to what information they can lawfully disclose if requested by a third party. I consider that providing certainty in the decision-making processes used by the parliamentary agencies in respect of information requests is of critical importance if we are to avoid the recurrence of the situation that is currently under consideration by the committee.

I consider that one option for achieving this certainty is to extend the Official Information Act 1982 ("OIA") to the parliamentary agencies, as proposed by the Law Commission in its recent review of the OIA. I suggest that consideration should be given to applying the OIA to the parliamentary agencies, but with the specific safeguards recommended by the Law Commission. Those safeguards include the exclusion of certain information (e.g. information about proceedings in Parliament, and members' and parties' information) from the scope of the OIA and the adoption of certain specific measures to prevent the operation of the OIA from impinging on parliamentary privilege.

In addition, I suggest that consideration should also be given to the extension of the Privacy Act 1993 in its entirety to the Parliamentary Service. The Law Commission recommended that the Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. It also proposed that information held by the Parliamentary Service on behalf of members should not be covered by the Privacy Act.

Currently, the Office of the Clerk is subject to the Privacy Act, but the Parliamentary Service is excluded from the application of that Act except in relation to personal information about current or former employees. Members are excluded in their official capacity, and the House of Representatives and the Parliamentary Service Commission are excluded entirely. Quite apart from the need to ensure consistency in the application of the Privacy Act between the Office of the Clerk and the Parliamentary Service, the underlying principles of that Act in relation to the collection, storage, use, and disclosure of personal information will provide helpful guidance to the Service on the proper management of any personal information that is held in the parliamentary information and security systems.

The Government has decided not to adopt the Law Commission proposals to extend the OIA and the Privacy Act to Parliament but the committee could recommend that the Government revisit those decisions.

While it would be possible for freedom of information principles to be applied to the House and appropriate protocols adopted, I believe that the OIA and the Privacy Act already contain adequate information management principles. Instead of reinventing those principles for use in the parliamentary context, the parliamentary agencies could be made subject to these statutes with safeguards such as those proposed by the Law Commission.

I intend to focus on the Law Commission's proposal to extend the OIA to the parliamentary agencies. I will begin by briefly describing the proposal. I will then discuss the current practice within the parliamentary agencies for dealing with information requests and conclude with a discussion of the advantages and disadvantages of the Law Commission's proposal.

Law Commission proposal

In its June 2012 report *The Public's Right to Know: Review of the Official Information Legislation*[1], the Law Commission recommended that the OIA should apply to the parliamentary agencies (the Office of the Clerk and the Parliamentary Service), and that in relation to each of these agencies the definition of "official information" should be limited to:

- statistical information about the agency's activities;
- information about the agency's expenditure of public money;
- information about the agency's assets, resources, support systems, and other administrative matters.

The Law Commission also recommended that the Speaker in his or her role as Responsible Minister for the parliamentary agencies under the Public Finance Act 1989 should also be included within the scope of the OIA.

[1] NZLC R125

The Law Commission's recommendations relate largely to information held by the parliamentary agencies about their operational and administrative activities. Information about the proceedings in Parliament is to be specifically excluded from the definition of "official information". The Law Commission made this deliberate policy choice after undertaking detailed discussions with the Office of the Clerk (which dated back to 2010) and taking into account a 2011 report of the Standing Orders Committee[2].

The Standing Orders Committee noted in its 2011 report that a great deal of parliamentary information is already available to the public through Hansard, the broadcasts of parliamentary proceedings, and the proactive release by select committees of all evidence received on an item of business. The Standing Orders Committee acknowledged the importance of openness and transparency in New Zealand's system of representative democracy, but considered that one option for a freedom of information regime for Parliament is to develop high-level principles established in legislation that are implemented under the Standing Orders or other rules adopted by the House or published by the Speaker. Such a regime would be similar to how the New Zealand Bill of Rights Act 1990 already applies to the legislative branch of government. At the core of the Standing Order Committee's concern was its uneasiness about any definition of "proceedings in Parliament" being included in the OIA (as this concept is at the heart of parliamentary privilege) which the Law Commission initially considered to be necessary in order to describe the scope of the proposed OIA regime for Parliament.

Following extensive discussions with my office, the Law Commission agreed not to apply the OIA to parliamentary proceedings in order to avoid the risk that extending the OIA regime to Parliament may impinge on parliamentary privilege. By limiting the information to be made subject to the OIA to information that relates to the internal functioning of the parliamentary agencies, the Law Commission has mitigated concerns about any adverse effect of the proposal on the ability of the House to maintain control over its own proceedings.

Now that it seems likely that a definition of "proceedings in Parliament" will be included in a Parliamentary Privilege Bill, the concern about an express reference in the OIA to excluding information about parliamentary proceedings is no longer so significant. However, it always has to be recognised that information about proceedings in Parliament may be, or may become, official information when in the hands of Ministers or their officials. This is a matter for departments dealing with OIA requests rather than Parliament, but the shifting status of such information does need to be borne in mind.

The Law Commission also recommended a number of other safeguards, intended to provide protection for members' and parties' information.

[2] Report of the Standing Orders Committee, *Review of Standing Orders*, I.18B, September 2011, see pp 63-65.

First, the Law Commission proposed that three types of information be expressly excluded from the definition of "official information" in relation to information held by a parliamentary agency:

- any information held by a parliamentary agency solely as an agent for, or on behalf of, the House of Representatives or a member of Parliament; and
- any information held by a parliamentary agency about a member of Parliament in relation to the member's performance of his or her role and functions as a member; and
- any information held by a parliamentary agency that relates to the development of political policies by a recognised party or an independent member of Parliament.

The Law Commission also noted that consideration should be given to whether the exclusions in the Freedom of Information Act 2000 (UK) that apply to individual members should also apply. These exclusions relate to information about:

- members' residential addresses and travel arrangements; and
- the identity of persons who deliver goods or provide services at a member's residential address; and
- members' security arrangements.

Secondly, the Law Commission recommended that a new provision in the OIA should state that nothing in the OIA limits or affects any privileges, immunities or powers of the House of Representatives.

Thirdly, the Law Commission recommended that the OIA should be amended to provide that the Ombudsmen must not recommend making available any official information held by a parliamentary agency or the Speaker, if the Speaker certifies that making the information available would be likely to limit or affect any privileges, immunities, or powers of the House of Representatives.

Current practice for handling information requests

Currently, the parliamentary agencies are not subject to the OIA. However, both the Office of the Clerk and the Parliamentary Service generally treat requests for information as if they were subject to the OIA in the interest of maintaining openness and transparency in their administrative operations, particularly in relation to the expenditure of public money.

By responding to information requests as if they were bound by the OIA, the parliamentary agencies can, and do, encounter several difficulties as a result.

First, the parliamentary agencies operate in a legal vacuum - they apply the OIA but are strictly speaking not bound by it. The corollary of this situation is that the parliamentary agencies also generally cannot take advantage of the machinery provisions in the OIA, such as the provisions dealing with the transfer of requests and consultation with interested parties. For example, if a parliamentary agency considers that the information to which a request relates is held by, or is more closely connected with the functions of, a

department or Minister, it cannot rely on section 14 of the OIA to formally transfer the request to the department or Minister in question because the OIA does not apply to it. Similarly, a parliamentary agency cannot rely on section 15(5) of the OIA to consult with a Minister or any other person about the proper disposition of a request.

More importantly, the parliamentary agencies cannot invoke any of the reasons specified in the OIA for refusing a request for information as those grounds technically do not apply to them. The parliamentary agencies therefore do not have any real practical experience in applying the reasons for withholding information under the OIA and as a result lack awareness of the interests or principles that underpin those reasons. Some of those principles (such as the protection of the privacy of natural persons, the maintenance of constitutional conventions which protect collective and individual ministerial responsibility, and the avoidance of contempt of the House) are particularly relevant and would have provided helpful guidance as to how the information requests from the Henry inquiry ought to be dealt with had the OIA applied to the parliamentary agencies at the critical time.

Secondly, parliamentary agencies do not have well developed systems in place for handling information requests. There has been no real incentive to develop such systems to the same degree as in the case of departments given that the parliamentary agencies are not subject to the OIA. As a consequence, the internal processes within the parliamentary agencies for dealing with information requests have generally arisen on an ad hoc and case by case basis. This in turn creates the risk that information requests are dealt with by various units within the parliamentary agencies, rather than by a central decision-maker. In contrast, every decision on a request under the OIA must be made by the chief executive of a department or a person authorised by the chief executive (see section 15(4)).

The absence of well-defined, systematic processes within the parliamentary agencies for handling information requests inevitably means that less rigour is being applied to decisions on requests than would otherwise be the case if the parliamentary agencies were subject to the OIA and such processes had to be developed and maintained. There is also a greater risk of inconsistencies in the decisions being made by parliamentary agencies in respect of information requests.

Advantages of applying the OIA to parliamentary agencies

If the Law Commission proposal to extend the OIA to the parliamentary agencies is implemented, it is likely to lead to the following outcomes:

- more structured procedures within the parliamentary agencies for handling information requests, including well defined decision trees and a centralised approach to decision-making:
- greater awareness within the parliamentary agencies of the interests or principles that underpin the OIA, including improved knowledge of the specific interests that are protected by the various statutory grounds for withholding information:

- access to the machinery provisions in the OIA which means that parliamentary agencies can transfer information requests if they consider that the information being sought is more closely connected with the functions of another agency, rather than having to deal with the requests first-hand:
- a better understanding within the parliamentary agencies that certain information is "out of bounds" such as members' and parties' information and should not generally be disclosed to a third party.

Disadvantages of applying the OIA to parliamentary agencies

Besides the additional administrative costs and resourcing issues that would inevitably arise from the Law Commission's proposal to extend the OIA to the parliamentary agencies, the exercise of the Ombudsmen's statutory investigative powers could impinge on parliamentary privilege. Under the Law Commission proposal, the Ombudsmen would have jurisdiction to investigate any complaint about the release of information under the OIA. This includes a broad power in section 19 of the Ombudsmen Act 1975 to require the production of any information which relates to a matter that is being investigated by an Ombudsman, and which is used in order for the Ombudsman to assess whether or not information is official information.

There is a risk that if the Ombudsmen become involved in adjudicating on complaints about the non-disclosure of information by the parliamentary agencies, they would require to see a copy of the information that was withheld to establish whether it is official information. This course of action could impinge on parliamentary privilege, especially if the information involved relates to parliamentary proceedings.

One option for mitigating this risk is for the House to consider making rules under section 15 of the Ombudsmen Act 1975. That section enables the House to make rules for the guidance of the Ombudsmen in the exercise of their functions under the Ombudsmen Act or the OIA. This guidance could include allowing for a procedural step in the investigation process, whereby members would have the opportunity to claim parliamentary privilege in relation to any information that is subject to the Ombudsmen's investigatory powers.

Another option for mitigating the same risk is already built into the Law Commission proposal and could be utilised if required. To deal with cases where there might be some doubt about whether proceedings of the House or parliamentary privilege may be involved in a request for official information made to a parliamentary agency, the Law Commission recommended that the Speaker should be given the discretion to certify that the release of the requested information would limit or affect any privileges, immunities, or powers of the House. The Speaker's certificate would then operate as a conclusive bar against the Ombudsmen recommending that the requested information be made available.

Finally, it needs to be noted that the Speaker's certificate would not necessarily cover member or party information which is not generally part of proceedings in Parliament. While such information is not intended to be official information, it seems inevitable that

there will need to be a mechanism for dealing with disputes over what constitutes member and party information. These will be matters for the member concerned as the owner of the information and it may be necessary for the Ombudsmen to become involved in deciding whether the information is official information, subject to any rules the House may consider necessary for the guidance of the Ombudsmen in the discharge of that function. Dealing with it this way should avoid the courts entering the fray.

I trust that these comments are of assistance.

Yours sincerely

Mary Harris
Clerk of the House of Representatives

Appendix – Responses to specific questions

> *Question 1 - How should information and security protection principles intended to safeguard data apply in a parliamentary context?*

In its reviews of the Official Information legislation and the Privacy Act, the Law Commission considered which agencies should be subject to these statutes and which should not, and made a number of recommendations about how the Official Information Act 1982 (OIA) and Privacy Act 1993 (Privacy Act) could be applied more effectively to parliamentary agencies. I consider that the Law Commission proposals are one option for applying information protection principles in a parliamentary context.

The Government in its response to the Law Commission recommendations did not agree with the proposals to extend the coverage of the OIA to the parliamentary agencies and supported the status quo.[3] It directed officials to carry out further work on the proposals to extend coverage of the Privacy Act.[4]

An alternative option would be to consider the adoption of high-level freedom of information principles established in legislation and implemented through Standing Orders or other rules adopted by the House or published by the Speaker, as recommended by the Standing Orders Committee.[5]

Official Information Act 1982

The Law Commission recommended that the OIA should apply to the Office of the Clerk of the House of Representatives and the Parliamentary Service, and that in relation to these agencies the definition of "official information" should include only:

- statistical information about the agency's activities;
- information about the agency's expenditure of public money;
- information about the agency's assets, resources, support systems, and other administrative matters.

The Law Commission recommended that the OIA should apply to the Speaker in his or her role as responsible minister for these agencies, and that the definition of "official

[3] Government Response to Law Commission Report on *The Public's Right to Know: Review of the Official Information Legislation.* Presented to the House of Representatives on 4 February 2013, at p3.
[4] Government Response to Law Commission Report on *Review of the Privacy Act 1993*. Presented to the House of Representatives on 27 March 2012, at p5.
[5] Standing Orders Committee *Review of Standing Orders* (September 2011) I.18B at 63-65.

information" should state that only information held by the Speaker in that capacity is included.

The Law Commission also recommended a number of safeguards, intended to provide protection for proceedings of the House of Representatives, and members' and parties' information.

First, that three types of information be expressly excluded from the definition of "official information" in relation to information held by a parliamentary agency:

- any information held by a parliamentary agency solely as an agent for, or on behalf of, the House of Representatives or a Member of Parliament; or
- any information held by a parliamentary agency about a Member of Parliament in relation to the Member's performance of his or her role and functions as a Member; or
- any information held by a parliamentary agency that relates to the development of political policies by a recognised party or an independent Member of Parliament.

The Commission also noted that consideration should be given to whether the exclusions in the Freedom of Information Act 2000 (UK) that apply to individual members should also apply. These include information relating to Members' residential addresses and travel arrangements, the identity of persons who deliver goods or provide services at a Member's residential address, and information on Members' security arrangements.

Secondly, that a new provision in the OIA should state that nothing in the OIA limits or affects any privileges, immunities or powers of the House of Representatives

Thirdly, that the OIA would be amended to provide that the Ombudsmen must not recommend making available any official information held by a parliamentary agency or the Speaker, if the Speaker certifies that making the information available would be likely to limit or affect any privileges, immunities, or powers of the House of Representatives.

Privacy Act 1993

Currently the Office of the Clerk is subject to the Privacy Act, but the Parliamentary Service is excluded except in relation to personal information about current or former employees. Members are excluded in their "official capacity", and the House of Representatives and the Parliamentary Service Commission are excluded entirely.

The Law Commission recommended that the Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held

by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Privacy Act.

Ombudsmen Act 1975

Under the proposals from the Law Commission set out above, the Ombudsman would have jurisdiction to investigate any complaint about the release of information under the OIA. This includes a broad power in section 19 of the Ombudsmen Act 1975 to require the production of any information which relates to a matter that is being investigated by the Ombudsman, and which is used in order for the Ombudsman to assess whether or not information is official information.

If the committee were to consider adopting the Law Commission proposals around the application of the OIA, it should also consider whether to recommend that the House use its power to make rules under section 15 of the Ombudsmen Act, to provide guidance for when the Ombudsman is investigating a complaint that relates to the Speaker or a parliamentary agency. This guidance could include allowing for a procedural step in the investigation process, whereby Members would have the opportunity to claim parliamentary privilege in relation to any information that is subject to the investigatory powers.

> *Question 2 - Are the information and personal privacy principles set out in applicable legislation (such as the Privacy Act, the Official Information Act, and the Evidence Act) relevant to the committee's inquiry in the context of parliamentary privilege? If so, which principles are relevant?*

The information and personal privacy principles set out in the OIA and Privacy Act are relevant to the committee's inquiry in the context of parliamentary privilege, because these statutes provide comprehensive guidance and a clear and consistent scheme for the handling of information. A lack of authoritative guidance about how to deal with information requests may have been a factor which contributed to the unauthorised release of information which gave rise to the need for the committee's inquiry.

Relevant principles in the Official Information Act 1982

The principles in the OIA which could be applicable include:

- the principle of availability in section 5;
- the various reasons for withholding official information in sections 6 and 9;
- the scheme for dealing with requests for official information, including the power to transfer requests where the information to which the request relates is not held or is more closely connected with the functions of another in section 14;

- the grounds for refusing an official information request set out in section 18, including refusal on the ground that the making available of the information would constitute contempt of the House of Representatives; and
- the exclusion from the definition of "official information" in section 2(1) of information held solely as an agent for a third party not subject to the OIA.

Relevant principles in the Privacy Act 1993

The principles in the Privacy Act which are relevant include:

- where an agency holds information solely as an agent, for the purpose of safe custody or for processing the information on behalf of another agency, and does not use or disclose the information for its own purposes, the information is deemed to be held by the agency on whose behalf it is held or processed (s3(4));
- the definition of "personal information" as information about an identifiable individual in section 2;
- the requirement for an agency to appoint privacy officers in section 23, whose responsibilities include dealing with requests and encouraging compliance with the information privacy principles;
- the good reasons for refusing access to personal information in section 27, 28 and 29; and
- the scheme for individuals to make information privacy requests relating to access to and correction of personal information in Part 5, including the power to transfer requests where the information is not held or is more closely connected with the functions of another agency in section 39.

The information privacy principles in section 6 of the Privacy Act are particularly relevant in this context. In summary, the principles are:

- collection of personal information only where necessary for a lawful purpose;
- collection of personal information directly from the individual concerned;
- the steps to be taken before personal information is collected;
- collection of personal information by lawful and reasonable means;
- secure storage of personal information;
- the right to have access to personal information held by an agency;
- correction of personal information held by an agency;
- accuracy of personal information to be checked before use;
- agency not to keep personal information for longer than necessary;
- use of personal information limited to the purpose for which it was collected;
- limits on the disclosure of personal information to third parties; and
- use of unique identifiers.

Principles in the Evidence Act 2006

The broad principle behind section 68 of the Evidence Act is that journalists should not be compelled to answer questions or provide documents that would disclose the identity of their sources, except where the public interest in disclosure of the identity outweighs any likely adverse effects on the source and the public interest in the news media accessing sources of facts and communicating facts and opinions to the public. This principle is relevant in the context of parliamentary privilege in a broad sense as it reflects the importance of the freedom of the press for our democratic system of government. However, section 68 is primarily intended to apply in a judicial context, and the provision specifically provides that it "does not affect the power or authority of the House of Representatives". Therefore it would not be suitable to apply this provision directly to the parliamentary context.

> *Question 3 - Should the collection and release of metadata information be treated differently from information which contains substantive content?*

For the reasons given below, it is proposed that the collection and release of metadata should not be treated differently from information that contains substantive content.

A. Definition of metadata

The committee's letter notes a definition of metadata.

The only definition of metadata in the statute book is found in the High Court Rules, in the glossary provided by Part 3 of Schedule 9, which relates to discovery.[6] The only uses of the term "metadata" in the statute book occur in Schedule 9. The definition is as follows:

> **"metadata** means data about data. In the case of an electronic document, metadata is typically embedded information about the document that is not readily accessible once the **native electronic document**[7] has been converted into an **electronic image**[8] or paper document, for example, the date on which the document was last printed or amended. Metadata may be created automatically by a computer system (system metadata) or may be created manually by a user

[6] *See* the High Court Rules, Schedule 9 ("Discovery checklist and the listing and exchange protocol"), Part 3 ("Glossary").

[7] The relevant definition is "**native electronic document** or **native file format** means an electronic document stored in the original form in which it was created by a computer software program".

[8] The relevant definition is "**electronic image** or **image** means an electronic representation of a paper document or electronically stored information. An electronic image may be a searchable image or an unsearchable image".

(application metadata). Depending on the circumstances of the case, metadata may be discoverable".

B. Similar concepts to metadata:

Call associated data is defined in section 3(1) of the Telecommunications (Interception Capability) Act 2004[9] as follows:

> **"call associated data**, in relation to a telecommunication,—
>
> (a) means information—
>
> (i) that is generated as a result of the making of the telecommunication (whether or not the telecommunication is sent or received successfully); and
>
> (ii) that identifies the origin, direction, destination, or termination of the telecommunication; and
>
> (b) includes, without limitation, any of the following information:
>
> (i) the number from which the telecommunication originates:
>
> (ii) the number to which the telecommunication is sent:
>
> (iii) if the telecommunication is diverted from one number to another number, those numbers:
>
> (iv) the time at which the telecommunication is sent:
>
> (v) the duration of the telecommunication:
>
> (vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but
>
> (c) does not include the content of the telecommunication."

C. Underlying concepts

If metadata is to be treated differently from substantive content, there needs to be a clear distinction between the two.

The distinction generally made is between information that is contained in a message ("substantive content"), and information about the message, especially about the container of the message. Thus, for example, who created and sent the message, when it was created or modified, who it was sent to, and when it was forwarded are matters that come within the meaning of "metadata".

---

[9] Section 3(1). The same definition is provided in the Act's successor, the Telecommunications (Interception Capability and Security) Bill, which is currently awaiting its second reading.

However, there is no commonality between understandings as to what exactly is and is not included in "metadata".

The distinction between metadata and substantive content appears to be based partly on the nature of the information each term represents, and partly on the concept that metadata information is not information that is essentially private or sensitive, and is therefore less in need of protection than substantive content.

D. Possible approaches

In the parliamentary context, the overriding consideration should be that metadata should not be treated in a way that would compromise the performance of members' representative functions, parliamentary proceedings, and any activities that are reasonably incidental to the discharge of the business of the House.

The difficulties of general uncertainty as to what is and is not meant by metadata would not prevent Parliament from defining "metadata" for uses relevant to information stored by the Parliamentary Service or by members, but a variety of definitions and rules may be needed for different applications, such as emails, telecommunications, voice mail, etc.

In this context, it should be noted that the definitions provided above have a simple core, but are not exhaustive. The expression of the simple core meaning is helpful for understanding the key concept, but not so much for delineating or limiting it.
If Parliament decided to define metadata (perhaps in several ways for different uses such as for email, voicemail, etc.), for the purposes of preventing data breaches, it may not be readily practicable to make the public aware of the ways the term is used in the parliamentary context. This could result in members of the public not being aware of what limitations or lack of them may exist in relation to wider dissemination of information around, for example, their communications with members of Parliament.

A series of relatively complex distinctions may be difficult to follow also for those required to handle release or requests for release of metadata. Errors could occur, and once released, information often cannot be recalled effectively.

More importantly, information that is metadata may be just as sensitive as substantive content, especially in the parliamentary context. Quite a lot can be learned from the revealing of metadata, such as the very existence and number of email communications from a member to a specified person. Subject lines and the names of attachments may also, for example, contain information that is as substantive as any content.

This does not indicate that substantive content should be treated with less care than, at least in principle, it is already. The suggestion is rather that however "substantive" content is to be treated, for example, in relation to consent for release, metadata should be treated in the same way.

> *Question 4 - Are there particular sets of information held on parliamentary information and security systems that should be treated differently from other information?*

Information of different types has to be treated according to restrictions that are appropriate for it. The more sensitive the information is, the greater the restrictions should be.

While there are various types and subjects of information that should be treated in different ways, there are relatively few sets of information as such that relate directly to those distinctions.

A. Types and subjects of information

There are many types and subjects of information held on parliamentary information systems and security systems. These include:

- Swipe card data from the use of personal access cards and car park cards
- Footage from parliamentary precinct CCTV
- Email, computer use, cell phone, land line, and voicemail metadata and content
- Paper records relating to applications for swipe cards, and to signing visitors in and out of the precinct
- Business records, including paper archives and electronic document filing systems (e.g. ECM)
- Party and individual political information
- Information on House and committee proceedings
- Information relating to election processes
- Information relating to lobbyists
- Information about member's expenditure on services and allowances
- Information relating to members' and Ministers' families and their services and allowances
- Information about travel by members
- Data relating to non-parliamentary agencies; for example the DIA
- Employment information (including payroll and HR information) relating to parliamentary and other staff.

See also the answer to Question 5 for further identification and analysis of the types and subjects of information held on parliamentary information systems and security systems.

B. Sets of information

Most of the types and subjects of information above are not held as "sets" of information. That is, they are not in separate and distinct storage systems or divisions of data.

Some types of information, while held as relatively distinct groups of information, are not held as sets of information about particular persons. An example of this is the security systems in the parliamentary complex, which consist of CCTV and the Cardax access system.

The Parliamentary Service considers that it is possible to distinguish between two sets of information that are derived from a number of systems that it maintains and manages and that collect and retain personal information[10]. The distinction that the Parliamentary Service makes between the two sets is as follows:

- The first set is information that is collected and stored because it is required to deliver and verify a service; for example, pay rates and entitlements information (so as to enable salaries to be paid), and expenditure information and tax receipts for the provision of financial services. In regard to this type of information, the Parliamentary Service considers that this set of information can be rightly thought of as belonging to the Service.

- The second type of information is information that is collected and retained as a by-product of a provided service; for example, email messages sent and received on the Parliamentary Service mail server, and phone log records about calls made on a phone provided by the Parliamentary Service. The Parliamentary Service considers that this set of information is a by-product of the service offered by the Parliamentary Service and should be considered as belonging to the user of the service, not the Parliamentary Service.

Another aspect of considering sets of information is that information relating to a member's different roles and interactions with others may not be held in mutually distinct ways or locations. For example, information relating to a member's role as a Minister may not be held as a separate set of information from other information about the member's interactions with his or her electorate constituents. Also, the information itself may overlap; for example, if a constituent consults the member in relation to a portfolio

[10] The approach taken by the Parliamentary Service may not be completely consistent with the approach that the Law Commission has suggested should be adopted under a revised Official Information Act 1982.

matter. Thus, there may not be a readily available "set" of information, because of a single storage place for several topics, or because the topics are not readily separable, or both.

The parliamentary precinct computer systems are maintained and operated by the Parliamentary Service. Internet servers may be used for material for more than one agency, so the information may be of a mixed parliamentary and non-parliamentary nature. There are also technical restrictions on retrieving and identifying some sets of information.

Other information does occur in "sets", such as employee information in relation to the parliamentary agencies. In addition, it is likely that it would be easy to retrieve from such sets specific information relating only to particular persons and topics.

Generally, deciding the status of a particular email[11] , and how it is therefore to be treated, will need to be done on a case by case basis, as storage sets available for parliamentary information and security system are limited and do not readily correspond to the need to recognise degrees of classification by reason of the information's sensitivity.

C. Should sets of information be treated differently?

One main distinction that needs to be made is whether information is of a type (for example, subject to parliamentary privilege) or subject (for example, personal information) that needs to be treated with a greater or lesser degree of confidentiality and what safeguards need to be in place in relation to it.

As the Law Commission indicated, in the parliamentary context, general law issues of privacy and official information would continue to require modification. While information relating to administrative matters could be made more available by some application of the OIA, this would be limited to statistical information about activities, and agency information about its assets, resources, etc. and its expenditure of public money. However, the Law Commission's proposed exclusion from "official information" of three types of information[12] will require certain sets of information to be treated differently.

---

[11] For example, whether it is for parliamentary purposes, written in a Ministerial capacity (and thus official information), for constituency purposes, party leadership purposes, or for electioneering.

[12] That is, any information held by a parliamentary agency -

- solely as an agent for, or on behalf of, the House or a member;
- about a member in relation to the performance of his or her functions as a member;
- that relates to the development of political policies by parties or independent members.

To the extent that the privacy laws and OIA already apply in the parliamentary context[13], or are treated as if they apply, the corresponding information requires also to be dealt with in the specified manner. Where it is possible to find a "set" of information that corresponds to a type or subject of information that requires special treatment, then that set of information can be treated accordingly.

As mentioned previously, it will often be necessary for an owner of information to view particular information and decide what type of information it is in terms of categories related to its sensitivity and treatment. Where such decisions are disputed, this raises the question of who resolves such disputes. In relation to a situation where privilege is claimed, it could, as suggested, be the Speaker by way of issuing a certificate. In other contexts, particularly if the OIA were applied, it may be the Ombudsman, where official information is involved, but this still leaves member and party information in question. Who that person or persons should be is the subject of further questions.

Question 5 - What is the status of information (including ownership) of the different types of information held on the Parliamentary information and security systems?

Types of information	**Holder**	**Where stored?**	**Owner**
Speaker's information	PS as agent	PS ICT	Speaker
Members: Constituency information	PS as agent	PS ICT	Member
Members: Personal	PS as agent	PS ICT	Member
Ministers: Portfolio responsibility	PS as agent	PS ICT	Member
Ministers: Personal	PS as agent	PS ICT	Member
Party: Operations	PS as agent	PS ICT	Whips
Party: Political Strategy	PS as agent	PS ICT	Party Leader
Proceedings of the House and committees	PS as agent	PS ICT	Clerk
House Administration	PS as agent	PS ICT	Clerk
Precinct Administration	Principal	PS ICT	GM

[13] For example, the application of the Privacy Act 1993 to the Parliamentary Service in relation to personal information about its employees.

Question 6 - How should collection and release of information relating to specific roles within the parliamentary context (such as Ministerial staff, members' staff, parliamentary staff, or journalists) be treated?

Specific role	**Current treatment of information**	**How should the information be treated in the future**
Ministerial staff	• employed by DIA • subject to OIA and Privacy Act	Continue to be subject to the OIA and Privacy Act.
Members' staff	• employed by the Parliamentary Service • not subject to OIA • subject to the Privacy Act in relation to personal information about current or former employees	OIA and Privacy Act could be applied in a limited way as recommended by the Law Commission. Disclosure will be subject to application of statutory grounds for withholding information.
Parliamentary Service Staff	• employed by the Parliamentary Service • not subject to OIA • subject to the Privacy Act in relation to personal information about current or former employees	OIA and Privacy Act could be applied in a limited way as recommended by the Law Commission.
Office of the Clerk Staff	• not subject to OIA • subject to the Privacy Act	OIA could be applied in a limited way as recommended by the Law Commission.
Staff of Department of Prime Minister and Cabinet	• subject to OIA and Privacy Act	Continue to be subject to the OIA and Privacy Act.
Parliamentary Counsel	• not subject to OIA • subject to the Privacy Act	No change proposed.
Journalists	• employed by various media organisations which are subject to the Privacy Act, but excluded for the purposes of news activities • subject to the Evidence Act 2006, s68 "Protection of journalists' sources	As private entities not covered by OIA, disclosure of Parliamentary Service-held administration system data will be subject to application of statutory grounds for withholding information.

	• subject to Rules of the Parliamentary Press Gallery	

Question 7 - Who should have authority over the release of information and how should that oversight be exercised?

Under the proposal to apply the OIA and Privacy Act set out above, authority and accountability for the release of information would sit with the chief executive of the relevant parliamentary agency to whom the request was made or transferred, or an officer or employee of that agency authorised by the chief executive (section 15(4) of the OIA and section 40(4) of the Privacy Act). The chief executive (or the authorised officer or employee) would also be able to consult with a Minister or any other person in relation to the decision (section 15(5) of the OIA and section 40(5) of the Privacy Act).

For example, if an OIA request was made to the Parliamentary Service, then the General Manager of the Parliamentary Service or an authorised employee of the Parliamentary Service could make the decision about whether to release or withhold the information, or to transfer the request (where the information is not held by the Parliamentary Service but is believed to be held by another department or Minister). That decision maker could, for example, consult with the Speaker and the Clerk where the request raised an issue of parliamentary privilege; and also with a member where the request related to them.

Question 8 - What thresholds or principles should apply to releasing this information, including where a security issue is cited?

Where the law requires that information be released, for example where the Police are executing a search warrant in respect of a criminal offence, or where a Commission of Inquiry has powers to compel the production of information, then these legal powers should continue to apply. The use of obtrusive powers such as these are generally only available where there is a significant public interest (for example a security interest) in the information being accessible, and there are checks and balances on their use. In this respect I am proposing that the status quo be maintained.

However, the proposal to apply the OIA and the Privacy Act would provide some thresholds and safeguards for the release of information in situations where the requestor does not otherwise have any legal authority to obtain access to the information.

The thresholds and principles that would apply to the release of information are those that are set out as reasons for withholding official information in sections 6, 7 and 9 of the OIA (as modified by the Law Commission proposal), the grounds for refusing an official information request set out in section 18 of the OIA (including refusal on the ground that the making available of the information would constitute contempt of the House of Representatives), and the reasons for refusing access to personal information in sections 27, 28 and 29 of the Privacy Act.

In relation to security issues, the reasons for withholding or refusing access that may be relevant include:

- that the disclosure of the information would be likely to prejudice the security or defence of New Zealand, or the international relations of the Government of New Zealand (section 6(a) OIA and section 27(1)(a) Privacy Act);
- that the disclosure of the information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial (section 6(c) OIA and section 27(1)(c) Privacy Act); and
- that the disclosure of the information would be likely to endanger the safety of any person (section 6(d) OIA and section 27(1)(d) Privacy Act).