



TCF Submission to:

**Department of the Prime Minister and Cabinet and
Ministry of Business, Innovation and Employment on**

DATA PRESERVATION CONSULTATION PAPER:

Towards accession to the Council of Europe Convention on Cybercrime

13 March 2019

A. Introduction

1. This submission is made by the New Zealand Telecommunications Forum Incorporated (**TCF**). The TCF is the telecommunications sector's industry body which plays a vital role in bringing together the telecommunications industry and key stakeholders to resolve regulatory, technical and policy issues for the benefit of the sector and consumers. The TCF enables the industry to work together and discuss issues and topics collaboratively, to reach acceptable solutions that can be developed and implemented successfully. Its members represent 95% of the New Zealand telecommunications industry by customer numbers.
2. This submission has been drafted in response to the Data Preservation Consultation Paper (**the Paper**) issued by the Department of the Prime Minister and Cabinet (**DPMC**) and Ministry of Business, Innovation and Employment (**MBIE**).
3. This submission provides general comment about the nature of the proposed regime. The Paper specifically asks for views about the costs of complying with the proposed preservation order regime. Views on the likely costs of compliance will be provided by individual operators, as their costs will differ.

B. Background

4. The New Zealand Government wishes to accede to the Council of Europe Convention on Cybercrime (referred to as the 'Budapest Convention'). Among other things, the convention requires New Zealand to have a 'data preservation scheme' which will require a new type of order which law enforcement can use (in addition to the existing search warrants, production orders, surveillance device warrants and examination orders).
5. The TCF notes that the Paper is not clear on the definition of a 'preservation order'. Consequently, the TCF seeks clarity on the regime and proposes that any process introduced should be the minimum that is needed to achieve the government's goal of being able to accede to the Convention.

C. Key Elements of a Preservation Order

6. The TCF understands that the rationale for preservation orders is to ensure that data which is likely to be the subject of a production order, and is at risk of being lost, is preserved until a production order can be obtained. It is understood that preservation orders will not require preserved data to be handed over until a valid production order is made.
7. The scope and breadth of preservation orders should not exceed the parameters of production orders. They should not allow agencies to request data to be preserved in predefined formats or require analysis of the data. They should not be able to circumvent the protections already in place to limit the extent of data able to be obtained by law enforcement agencies. Any increase in the breadth of data which can be the subject of a preservation order would be an expansion in the reach of law enforcement agencies and should be the subject of broader public consultation.
8. Preservation orders should apply only to the data that is captured and exists as part of the Telecommunications Operators' usual business activities. Preservation orders should not be used to require operators to create active measures to capture and store data that otherwise would not be captured. In other words, Preservation orders should not be used in the situations where a Surveillance Device Warrant is required (as a form of "delayed proactive lawful intercept").
9. The threshold for obtaining preservation orders needs to be set at the appropriate level. A low threshold, particularly in the case of forward-looking preservation orders would effectively sanction 'fishing expeditions'.
10. There is a cost associated with retaining data on behalf of law enforcement agencies. Therefore, the duration of preservation orders should be appropriately limited. The

purpose of preservation orders is to temporarily preserve data in order to allow law enforcement agencies time to obtain a production order. Preservation orders should not be used to hold data indefinitely in case it might prove useful at a later date. Use of preservation orders in this way would be inconsistent with the purpose of preservation orders, and with broader data protection legislation.

11. The TCF agrees with the proposal in the Paper that the likely costs associated with preservation orders will include:
 - i. time and resources to receive and check an order;
 - ii. infrastructure to hold stored data;
 - iii. Processing capacity to copy and store the data; and
 - iv. Other compliance and staffing costs
12. It should be noted that if a subsequent production order for the data is made which is narrower or in different terms to the preservation order, the preserved data set will need to be manually edited to comply with the terms of the production order. Complexities such as these increase the risk of data error and will increase the cost of compliance as significant resources will be required to comply with the production order, beyond the cost of preservation.
13. The extent of data to be preserved must not be greater than the data actually required by the agency. Preservation orders must not be able to be used to require large quantities of data to be held on the off-chance it might be useful.
14. Preservation orders should apply only to data which would be lost within the time frame that a final production order would be provided. This is because the production order itself can request data that has not been lost. Therefore, preservation orders should apply only to situations where, in the absence of such an order, the data could reasonably be anticipated to be lost.
15. Preservation orders should not be used as a means of capturing data that may be produced in the future. Forward looking production orders are available under the Search and Surveillance Act and these powers offer an appropriate means of obtaining and preserving data which may be produced in the future.¹
16. The Paper notes that the Police currently contributes to the cost of compliance with production orders. This highlights that the current processes for cost recovery in relation to production orders differ between the many agencies that make use of these orders. Given the higher anticipated costs associated with preservation orders, the TCF

¹ Search and Surveillance Act 2012, s 71(2)(g)(ii).

supports a single cost recovery process which applies to preservation orders, regardless of the agency issuing the order.

17. Telecommunications operators retain customer data for business purposes and to provide services to their customers. An obligation to retain data for longer than normal business requirements may expose the operators to legal risks associated with obligations to protect their customers' data. Consequently, the TCF expects that the requirement to comply with preservation orders will allow operators to balance customer data protection obligations with their obligations to law enforcement agencies.

D. Conclusion

18. The TCF understands the Government's desire for preservation orders, however, they must not extend the reach of law enforcement agencies or allow large quantities of data to be held for extended periods, just in case it is required in the future. The role of preservation orders is to enable law enforcement agencies to apply to preserve specified data for a short period pending a production order.
19. We anticipate potentially significant costs associated with the implementation and maintenance of a data preservation scheme. These costs must be recoverable under a single cost recovery scheme regardless of which agency has requested the order.
20. The TCF is happy to answer any questions the DPMC or MBIE might have on the views set out in this submission.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'G. Thorn', followed by a horizontal line.

Geoff Thorn
Chief Executive Officer
New Zealand Telecommunications Forum (TCF)