Chapter 9 – Production orders

BACKGROUND

9.1 Prior to the Search and Surveillance Act 2012 (the Act), enforcement officers who wanted to obtain data from a third party, such as a telecommunications company or a bank, would obtain a standard search warrant.[1] While search warrants are normally executed by the applicant actually searching the premises for the evidence him or herself, the common law provided that where the thing to be seized was held by a cooperative third party, the warrant could be executed by merely sending the warrant to the organisation named.[2]

9.2 In its 2007 Report, *Search and Surveillance Powers*, the Law Commission recommended introducing a specific form of authorisation for these types of searches – to be called production orders. The main rationale for these orders was that it is easier for the person against whom the order is made to locate the information than it is for the enforcement officer.[3] It will generally be less disruptive to a third party business to comply with a production order than with a standard search warrant and it will usually reduce the amount of irrelevant material seen by the enforcement officer.[4]

9.3 The Commission noted a number of potential disadvantages of introducing production orders – namely, that it may add complexity to the search regime and be confusing to have two processes for the same information.[5] However, ultimately it thought that a production order would better reflect the nature of the transaction and would provide a less intrusive form of search power.

---

1 In this chapter, we use the term "third party" to refer to the entity against which a production order is made. While production orders are usually made to obtain information about a person who is a customer of an organisation against which the order is made, it is possible for them to be made against any person or entity, including against a person who is a suspect or later becomes a suspect.

2 *R v Sanders* [1994] 3 NZLR 450 (CA).

3 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.18].

4 In its final report on the Search and Surveillance Bill, the Select Committee noted that there had been some misunderstanding about the nature of the production order regime and that they were intended to provide a less intrusive alternative to a search warrant in circumstances where the party subject to the order was willing to cooperate with enforcement officers: Search and Surveillance Bill 2010 (42-2) (select committee report) at 11.

5 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.20].

9.4 The Commission also considered whether there should be a lower threshold for issuing production orders for specific types of information, such as account holder information from financial institutions. However, it did not recommend a lower threshold because it thought there was nothing to distinguish that type of information from other types of information and a lower threshold would be seen as sanctioning fishing expeditions.[6]

Current law

9.5 The Act generally reflects those recommendations. It states that any enforcement officer who has a power to apply for a search warrant in respect of documents may apply for a production order for those documents.[7] He or she must have reasonable grounds to:[8]

- suspect that an offence has been, is being or will be committed (being an offence for which that officer may apply for a search warrant); and
- believe that the documents constitute evidential material in respect of the offence and are in the possession or under the control of the person against whom the order is sought (or will come into their possession or under their control while the order is in force).

9.6 This threshold for the issuing of production orders is equivalent to the threshold for search warrants. Also, as with search warrants, the section *empowers* the enforcement officer to get a production order, rather than specifying when he or she *must* get one. However, unlike a search warrant, which provides a power for the enforcement officer to search for the targeted material him or herself, a production order requires the third party to provide the information. If the third party fails to comply with the order without reasonable excuse, that person or entity is liable on conviction to a term of imprisonment not exceeding one year (for an individual) or a fine not exceeding $10,000 (for a body corporate).[9]

9.7 It should also be noted that a production order under the Act may be made against *any* person. That could be an individual or a legal entity, or even a suspect. It is not limited

---

6 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.26].

7 Search and Surveillance Act 2012, s 71.

8 Section 72.

9 Section 174.

to commercial companies and there is no condition that the person or company is considered to be cooperative.

9.8 Many of the provisions relating to search warrants also apply to production orders. In particular:

- the issuing officer may require the applicant to supply further information;[10] and
- applications must generally be in writing but the issuing officer may allow an oral application to be made (for example, by telephone) if the required information is supplied, the issuing officer is satisfied that the delay caused by a written application would compromise the effectiveness of the search, and the matter can be properly determined orally.[11]

How production orders are used

9.9 Production orders are one of three mechanisms by which enforcement agencies can obtain information from a third party. The other two mechanisms are by voluntary disclosure and by other statutory powers. Under the voluntary disclosure mechanism, an agency simply requests the information from the third party without relying on any legal authority, just as it can ask questions of any person who may have relevant information about offending.[12] It is up to the third party to decide whether it will voluntarily release the information. Where the information sought is personal information, an information privacy principle under the Privacy Act 1993 permits its release to an enforcement officer if:[13]

> … it is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

9.10 It is important to be clear that this principle does not empower the enforcement agency to ask for the information. It merely permits the third party to release it. We also note that a third party company that receives regular requests for customer information from enforcement agencies may have an agreed protocol or Memorandum of Understanding with the agency covering what type of information the company will voluntarily release and what it will require a court order for.

---

10 Search and Surveillance Act 2012, s 73(2)(a).

11 Section 73(2)(c).

12 *R v Thompson* (1995) 13 CRNZ 546 (HC).

13 Privacy Act 1993, s 6, principle 11(e).

9.11 There are a number of statutory provisions that empower agencies to request information from third parties for law enforcement purposes. Some of those powers require a court order,[14] but many are exercised on the authority of a person acting under the relevant Act. This latter category includes:[15]

- section 17 of the Tax Administration Act 1994, which enables the Commissioner of Inland Revenue to require any person to provide information or produce documents for inspection which the Commissioner considers necessary or relevant for the administration or enforcement of any of the Inland Revenue Acts or any other function of the Commissioner;[16] and
- section 11 of the Social Security Act 1964, which enables the Chief Executive of the Ministry of Social Development to require any person to provide information, produce documents or furnish copies or extracts of a document or record for a range of purposes under that Act, including determining whether a person claiming a benefit is entitled to receive that benefit.[17]

9.12 Production orders are used by many government agencies with law enforcement functions, including New Zealand Police, the Department of Internal Affairs and the Ministry for Primary Industries. Examples of how they are used include:

- in a child pornography investigation, to obtain the IP address of a suspect;
- in an animal welfare investigation, to obtain the animal's health records from the suspect's veterinarian;
- in a fisheries investigation, to obtain the bank records of a person suspected of illegally selling fish.

Any enforcement officer who can apply for a search warrant can also apply for a production order.

---

14 For example, s 42 of the Fair Trading Act 1986 enables the Commerce Commission to apply to a court for an order requiring a person to disclose information if the court is satisfied the person has engaged in conduct contravening Parts 1 to 4 of that Act.

15 Privacy Commissioner *Transparency Reporting Trial Aug–Oct 2015: Full Report* (2016). Appendix B lists 51 information gathering powers under a variety of statutes, but not all of these relate to law enforcement purposes.

16 See *New Zealand Stock Exchange v Commissioner of Inland Revenue* [1990] 3 NZLR 333 (CA).

17 See *Reed v R* [2014] NZCA 525 at [32]–[37].

9.13 Agencies do not routinely publish statistics on the number of requests they make for information from third parties – whether by production order or other mechanisms.[18] However, a recent trial of transparency reporting by the Privacy Commissioner provides an indication. This trial follows an emerging international trend for large telecommunications and internet companies to publish transparency reports. Those reports provide statistics on the number and nature of requests received by a company from government agencies for personal information about their customers.[19]

9.14 The Privacy Commissioner's trial, which ran across a three-month period (August to October) in 2015, was designed to better understand how it could assist companies in this type of reporting. Ten companies agreed to produce standardised transparency reporting information. They included two telecommunications companies, seven financial services companies, and one utility company.[20]

9.15 In summary, the Privacy Commissioner reported that over the three-month trial period:[21]

- the participants received 11,799 requests for customers' information;
- 11,349 of those requests were accepted in full, one was partially accepted and 449 were declined; and
- the bulk of requests came from Inland Revenue (4,670 requests), Police (3,513 requests), and the Ministry of Social Development (3,150 requests).

9.16 The trial found that 962 requests were made under a production order (that is, approximately 8 per cent of the total requests) and roughly twice as many were by voluntary disclosure. The majority were made under statutory powers of authority, particularly section 17 of the Tax Administration Act or section 11 of the Social Security Act.[22]

---

18 Below at paragraph [9.60] we ask whether enforcement agencies should be required to report annually on the number of production orders for which they apply.

19 Wikipedia, The Free Encyclopedia "Transparency Report" <https://en.wikipedia.org/wiki/Transparency_report>. We also note that in New Zealand, Trade Me began publishing an annual transparency report in 2013, detailing requests for information from Police, other government departments and the Disputes Tribunal. Trade Me's transparency reports can be found at <www.trademe.co.nz/trust-safety/2016/7/22/trade-me-transparency-report-2016/>. We are not aware of any other New Zealand companies that are currently publishing this type of data.

20 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 11.

21 At 13.

22 At 28.

9.17 This trial gives us an indication of how production orders fit into the range of mechanisms available to government agencies for obtaining information from third parties.[23] It is not a reliable indicator of the number of production orders made (because the ten companies involved in the trial represent only a subset of all the companies from which information may be sought under a production order). It should also be noted that requests for information under the other mechanisms will, in some cases, be for non-law enforcement purposes (for example, finding missing persons).

9.18 We have been told by enforcement agencies that, in practice, the choice of mechanism that is used to obtain information will depend upon a number of factors, including:

- the stage of the investigation;
- the nature of the information sought and whether the officer considers that a request for it may invade reasonable expectations of privacy; and
- prior knowledge of the requirements of the third party from whom it is sought.

9.19 In many cases, voluntary disclosure of information is sought when the investigation is still at an early stage and the thresholds for a production order cannot be met. That is, there may not yet be reasonable grounds to suspect that an offence has been, is being, or will be committed, nor reasonable grounds to believe that the documents sought are in the possession or control of the person against whom the production order would be made. In the earlier stages of an investigation, Police will sometimes not know what information is held or by whom it is held.

9.20 In other cases, officers make an assessment as to whether the information sought may later be held to have been improperly obtained and perhaps be ruled inadmissible as evidence in criminal proceedings under section 30 of the Evidence Act 2006. If that is a concern, there is an incentive to apply for a production order. In effect, officers assess whether the information request may be considered to invade reasonable expectations of privacy. Generally, the more invasive the information sought, the more likely that either the third party will require a production order or the enforcement officer will seek to protect the future admissibility of the information by applying for a production order.

---

[23] In addition, Trade Me's 2015 transparency report states that in that year, the greatest number of inquiries for personal information came from Police (1,840 inquiries), the Ministry of Business, Innovation and Employment (175 inquiries), the Ministry of Social Development (95 inquiries) and the Commerce Commission (91 inquiries).

9.21 A number of issues arise from these legal and practical aspects of production orders:

- whether the Act should be clearer about when a production order is required;
- whether enforcement agencies should be required to report on the number of production orders they apply for; and
- whether people should be notified when their information is sought from a third party by a production order.

9.22 We discuss each issue in turn.

SHOULD THE ACT BE CLEARER ABOUT WHEN A PRODUCTION ORDER IS REQUIRED?

9.23 We have encountered some concern (noted in the Privacy Commissioner's report on its transparency trial)[24] that enforcement officers are sometimes obtaining information by voluntary disclosure when it is thought they should be applying for a production order.[25] They are able to choose to request the voluntary disclosure of information because the Act does not specify when a production order must be obtained. The question for this review is whether the Act should be clearer as to when a production order is required.[26]

9.24 The types of information sometimes obtained by enforcement officers by voluntary disclosure include:

- electricity consumption data from an electricity supplier;
- airline travel information, including immediate and future travel plans;
- identification details from a company's customer database, linked to a telephone number or email address supplied by the enforcement agency; and
- metadata associated with the use of a phone (for example, indicating which cell phone sites the phone has linked to and when that occurred).

9.25 This issue is really a subset of the broader issue discussed in Chapter 2 as to whether the Act should be more specific about when a prior authorisation for any type of

---

24 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 6.

25 See also David Fisher "Police Given Personal Information Without Search Warrants" *The New Zealand Herald* (online ed, Auckland, 25 March 2015); and Nick Grant "Hager Adds New Claim in Action Against Police" *The National Business Review* (online ed, Auckland, 5 April 2016).

26 We note that the Supreme Court is currently considering a case that raises issues about the use of requests for voluntary disclosure instead of production orders. The case is subject to suppression orders until final disposition of the trial.

search is required.[27] As was explained in that chapter, the Act also does not specify when a search warrant is required.

9.26 This issue arose in the context of a police investigation into the identity of the person known as "Rawshark", who supplied information to journalist Nicky Hager for his book *Dirty Politics*. As we described in Chapter 8, Police were investigating the identity of "Rawshark" and whether he or she had committed an offence by unlawfully accessing the computer of blogger Cameron Slater. In pursuing this investigation, Police sought information about Mr Hager from a number of banks, telecommunications companies and airlines without first obtaining a warrant or production order. Most refused the request but one bank complied and provided details of Mr Hager's accounts.[28] There was considerable public interest in this story with several commentators questioning whether Police should be able to request this type of information without a warrant or production order, and whether a bank should be able to supply it.[29]

Possible concerns with the current approach of the Act

9.27 The current approach in the Act of empowering enforcement officers to apply for production orders rather than describing when they must be obtained could be seen as having a number of disadvantages.

Lack of clarity and consistency about when the Act should be applied

9.28 By not specifying when a production order is required, the Act leaves that decision to enforcement officers and the people who hold the information (usually a third party). In the absence of specific guidance in the Act, there appears to be a broad spectrum of opinion as to when a production order is required. Some consider that by enacting a production order regime in the Act, Parliament must have intended that it be used for every request. Others consider that the words of the statute cannot be interpreted as

---

27 See paragraph [2.89] above.

28 David Fisher "Police Got Hager Data Without Court Order" *The New Zealand Herald* (online ed, Auckland, 24 October 2015).

29 Rick Shera "Privacy Implications of Westpac's Release of Nicky Hager's Personal Information" *The National Business Review* (online ed, Auckland, 31 October 2015); Shannon Gillies "Westpac Under Fire for Hager decision" *Radio New Zealand* (online ed, Wellington, 28 October 2015); and Anthony Robins "Angry at Westpac" (26 October 2015) The Standard <https://thestandard.org.nz/angry-at-westpac/>.

overriding the enforcement officer's freedom to ask for any information by voluntary disclosure.

9.29 Described in another light, this is a question as to whether the principle in *R v Thompson* remains good law since the enactment of the Act.[30] In that case, Police obtained electricity consumption information from an electricity supplier without a warrant. The Court of Appeal said that it was not unlawful for the police officer to make the inquiry without a warrant and for the electricity supplier to supply the information. It held that the disclosure "came squarely within exception (e) of Principle 11 of the Privacy Act 1993".[31] We consider that, in the absence of clear guidance from the Act as to when a production order must be obtained, it is not clear whether *Thompson* remains good law and, accordingly, when a production order must be obtained.

Officers applying reasonable expectations of privacy test

9.30 It may be thought that enforcement officers are not well-placed to determine whether a production order should be applied for in individual circumstances. As described above, one of the key considerations when they make that decision is whether obtaining the information would invade reasonable expectations of privacy. However, as we described in Chapter 2, determining whether a search (or in the case of a production order, a request for information) might invade reasonable expectations of privacy will often involve a highly nuanced assessment. It may be unrealistic to always expect enforcement officers to make that assessment accurately.

Retrospective recognition of rights

9.31 Another concern might be that by leaving the determination as to whether a production order is required to the enforcement officer, the Act provides little proactive protection of privacy rights. If the enforcement officer gets it wrong, the main way for a person to challenge the decision of the enforcement officer is to challenge the admissibility of

---

30 *R v Thompson* (2000) 18 CRNZ 401, [2001] 1 NZLR 129 (CA).

31 At [54]. Principle 11(e) of the Privacy Act 1993 provides (amongst other things) that an agency holding personal information may disclose that information to a person, body or agency where the agency believes on reasonable grounds that this is necessary "to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences". This aspect of the decision was not discussed in Law Commission *Search and Surveillance Powers* (NZLC R97, 2007).

the information if it is introduced as evidence in proceedings. That may amount to a fairly weak protection of rights because it occurs a considerable time after the information is supplied and such a challenge can only be mounted in relation to information that becomes evidential material.

9.32 In contrast, if the Act describes when a production order is required, the request for information covered by that provision would be subject to an issuing officer's consideration as to whether the threshold for making a production order is met.

9.33 In theory, it may also be possible to judicially review a decision to obtain information by voluntary disclosure rather than by production order. However, this would only provide retrospective recognition of rights and, in any event, the courts have been concerned about the use of judicial review proceedings to challenge search warrants prior to criminal charges being laid. Similar concerns may apply to any challenge to a decision to seek information without a production order.

9.34 In the leading case, *Gill v Attorney-General*, Dr Gill challenged a warrant authorising a search of her medical practice by way of judicial review.[32] The challenge occurred when the investigation was still proceeding and before any criminal charges had been laid. It had the effect of temporarily halting the investigation. The Court said that the issues arising under that challenge—relevance and the admissibility of evidence—would be more appropriately dealt with as direct challenges to the admissibility of evidence once charges were laid. It indicated that judicial review should be reserved for cases where:[33]

> … the defect in the search warrant is of a fundamental nature, where the matter could be said to go to the jurisdiction of the issuing officer or where some other ground of true unlawfulness (such as want of jurisdiction) is established.

9.35 This principle was recently applied in *Hager v Attorney-General* where the High Court observed that an application for judicial review should not be entertained unless it is a clear case of an unlawful search and seizure of a fundamental kind.[34] It therefore appears that in the absence of statutory rules about when a production order must be obtained, it would be a very rare case where a request for the voluntary disclosure of information could be challenged by judicial review.

---

32 *Gill v Attorney-General* [2010] NZCA 468, [2011] 1 NZLR 433.

33 At [20].

34 *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523.

Third parties as decision-makers

9.36 As we described above, it can be the third party against whom a request for information is made that determines whether or not a production order is required. In our view, arguably these third parties are also not well-placed to be making that decision.

9.37 When a third party is making that decision, it will often be applying the exception in the Privacy Act 1993 to the usual rule of non-disclosure of personal information – that disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency.[35] Some possible concerns with this type of decision include:

- the threshold is too low (it is obviously lower than the threshold for making a production order);
- decisions about disclosure of information should be made by a publicly accountable decision-maker rather than the holder of the information, on the basis that the holder has motivations that may conflict with the protection of the privacy interests of its customers; and
- these third parties might not have sufficient information to determine whether disclosure is necessary in the circumstances.

9.38 On this final point, we have heard anecdotally (from people we have had preliminary discussions with) that sometimes very limited details of the investigation are provided when requests for personal information are made without a production order or warrant. At the very least, it is likely that there are a variety of practices across the thousands of requests for information without a production order or warrant for law enforcement purposes that are made every year. Also, there is likely to be a range of views as to the type of assessment that should be conducted before being satisfied that disclosure is necessary.

9.39 Interestingly, one commentator on the *Hager* case pointed out that police requests for information from third party organisations look very official – they contain the police crest, are set out like a legal document and contain formal language. The implied

---

[35] Privacy Act 1993, s 6, principle 11(e). See footnote 31 above.

concern is that it may not be clear to a less sophisticated third party that they have an option to decline the request.[36]

Advantages of the current approach

9.40 Despite the concerns outlined above, there are also a number of advantages to the current approach, which gives enforcement officers the option to seek information from third parties either on a voluntary basis or via a production order.

Avoiding cost and delay

9.41 The biggest advantage to enforcement officers is that the approach enables greater efficiency in investigations. If the Act requires more requests for information to be made only with a production order, that would have a significant impact on costs and delay in investigations.

9.42 Police and other enforcement agencies rely heavily on the voluntary provision of information for much of their work. Together, they make tens of thousands of requests for information on a voluntary basis from third party organisations every year. For example, Police told us that:

- in a recent 12-month period there were 29,750 requests for information to telecommunication companies in relation to 111 emergencies,[37] attempted suicides, firearms incidents, kidnappings and child abductions, bomb threats and threats to kill;
- on 25 April 2016 there were 3,499 "agreed Child Protection Protocol" cases, meaning that Police and Child, Youth and Family were jointly investigating allegations of serious child abuse and voluntarily sharing information under the Privacy Act.[38]

9.43 Police tell us that an application for a production order can take four to six hours to prepare and obtain from an issuing officer. It could be shorter if the enforcement officer has easy access to a court house, but longer (sometimes several days) for more complex applications. Applications are usually in writing. There is provision for them

---

[36] Rick Shera "Privacy Implications", above n 29.

[37] See for example *Arnerich v R* [2012] NZCA 291 at [18].

[38] Police also have Approved Information Sharing Agreements with the Inland Revenue Department and the Ministry of Social Development under which personal information is voluntarily shared in reliance on the exceptions in the Privacy Act 1993.

to be made by telephone call or by personal appearance, but first the issuing officer must be satisfied that:[39]

- the delay caused by requiring a written application would compromise the effectiveness of the search;
- the question of whether the production order should be issued can properly be determined on the basis of an oral communication or a personal appearance; and
- all the necessary application information in section 98(1)–(3) is supplied.

9.44 Even an oral application for a production order would require significantly more time to gather the requisite information than an informal request based on voluntary disclosure.

Enabling provision of evidence

9.45 We are told that many requests for the voluntary disclosure of information are made at a point in the investigation at which enforcement officers do not have sufficient evidence to support an application for a production order. There is a concern that statutory amendments to require production orders for those types of requests would prevent some investigations from proceeding. Frequently, information obtained from third parties by voluntary disclosure provides the evidence to meet the threshold requirements for obtaining a subsequent search warrant or production order. For example, an enforcement officer might ask an organisation to voluntarily disclose whether a person is a customer so that they can then obtain a production order against that organisation for the customer's information. If more requests for information require a production order, it is feared that investigations will not be able to proceed because the thresholds could not yet be met.

9.46 Similarly, in many instances a person or entity providing information voluntarily is a witness to the offending or is able to supply a record of it occurring. Examples include a bystander who sees an assault occur or a service station that supplies video footage of a robbery occurring on its premises. It cannot be envisaged that a production order would be required before that type of information is supplied. It is and has always been part of the core role of Police to speak to witnesses and victims of crime to piece together information about what has occurred.

---

[39] Search and Surveillance Act 2012, s 100(3).

Enabling more refined requests

9.47 We have encountered an argument that requests for information on a voluntary basis may be less intrusive of privacy than requests based on compulsion under a production order or other statutory power. If the request is received informally, the organisation can evaluate the precise nature of the information required for the investigation and only supply that. A production order will include a description of the information required to be produced, which will often be somewhat broader in scope than the precise information required.

9.48 Trade Me made this point in its 2016 Transparency Report:[40]

> In many ways, it's better for our members when we work under the Privacy Act as it gives us the ability to better control the amount and relevance of information released. This ensures irrelevant member data isn't caught up in the release and the requester only gets what's really useful. Put another way, this approach allows us to use a scalpel rather than a chainsaw.
>
> Compulsion orders, on the other hand, can be wide in scope and will often require the release of information that may not be directly relevant to the matter under investigation. We're legally required to comply with compulsion orders, regardless of scope.

9.49 The report gave the following example:[41]

> … if [the Ministry of Business, Innovation and Employment] was investigating a car seller to determine if they should be registered under the Motor Vehicle Sales Act, a Privacy Act release would allow us to only release sales data that covered motor vehicle sales, not the seller's full sales history which could be legally required under a compulsion order.

9.50 This is an interesting point. However, we consider it can only be argued that voluntary disclosure is a better method than compulsion for minimising the risk of disclosing irrelevant data when the organisation holding the information has a strong interest in protecting the privacy of its customers. Where that is not the case, it could be argued that compulsion (and therefore, consideration of the threshold by an issuing officer) is a better method. Also, Trade Me's concern could also be addressed if production orders were more specific in the description of the information sought.

Options for reform

9.51 If it was thought that the Act should be clearer about when a production order is required, the Act would need to define what types of information requests that rule

---

[40] Trade Me *Transparency Report* (2016) at 4, available at <www.trademe.co.nz/trust-safety/2016/7/22/trade-me-transparency-report-2016>.

[41] As above.

applies to. It is not contemplated that Police should never obtain information by voluntary disclosure, or else Police could not talk to potential witnesses.

Reasonable expectations of privacy

9.52 In Chapter 2 we discussed whether the Act should introduce a mandatory residual warrant regime or require authorisation for all search and surveillance activities and, if so, how the Act should define the conduct covered by such provisions.[42] We offered two options for defining what conduct should require prior authorisation (whether by a warrant, statutory power or other form of authorisation):[43]

- conduct that invades a reasonable expectation of privacy; or
- an alternative two-part test focusing on the type of information sought and whether it is publicly available.

9.53 If the Act were amended to require authorisation for all search or surveillance activities falling within either of those definitions—or any other definition developed—that test could also apply to information sought from third parties. In that case, it may not be necessary to have a separate test that sets out when production orders are required. If it was not considered appropriate to require a production order for all requests for information falling within the definition, the Act could specifically permit voluntary disclosure in certain circumstances.

9.54 Alternatively, whether or not that type of amendment was made, the Act could be amended to include a specific test for when a production order must be obtained. We have developed two further possible options.

Type of entity from which it is requested

9.55 The Act could state that a production order is required for certain types of information from certain types of entities. Those descriptions could be either general or specific. For example:

- any documents held by any person or entity that holds the information sought in the normal course of business; or
- any documents held by the following types of goods or service providers:

---

42 See paragraphs [2.89] and [2.105] above.

43 See paragraphs [2.107] and [2.112] above.

- telecommunications service providers;
- internet service providers;
- financial services providers;
- electricity and gas suppliers; or
- transport services providers.

9.56 The disadvantage of this option is that it is somewhat arbitrary. It does not capture with precision all requests for information that may invade a reasonable expectation of privacy. It is likely to capture either too many requests (and therefore have an unjustifiably chilling effect on law enforcement investigations) or too few requests (and therefore provide insufficient protection of privacy interests).

Production orders as the default position

9.57 Another option is for the Act to state that enforcement officers must obtain a production order, if it is possible to do so without prejudicing the investigation. In effect, this would make production orders the default position and enforcement officers would have to show that they had good reasons related to the investigation for not obtaining a production order.

9.58 However, this option may be of limited utility. It is likely that the majority of requests for voluntary disclosure of information would be made:

- under time pressure because the information sought (or evidential material that might flow from that information) might be lost or deleted; or
- where the thresholds for a production order could not yet be reached.

9.59 In both these cases, obtaining a production order would not be possible and so a request for voluntary disclosure of information could be made. It is likely that the only cases captured by this test would be those where there is no time pressure or the investigation has advanced to the point where the threshold for a production order is met.

Q41 Should the Act specify when a production order must be obtained?

REPORTING REQUIREMENTS

9.60 It has been suggested to us (from people we have had preliminary discussions with) that the Act should require enforcement agencies that use production orders to report

annually on the number they have applied for, as they are required to do in relation to other orders.

9.61 Currently, the Commissioner of Police and the Chief Executive of any enforcement agency exercising search or surveillance powers under the Act are required to report annually on their use of warrantless powers for entry, search or surveillance; surveillance device warrants; and declaratory orders. They must report the numbers granted or refused in the relevant year and provide certain details about the nature of the orders made.[44] Police are also required to provide similar information about examination orders.[45]

9.62 These requirements followed similar recommendations in the Law Commission's 2007 Report.[46] The Commission said that this type of reporting serves two purposes:[47]

> … it provides a layer of accountability by providing information to Parliament on the exercise of coercive powers specifically authorised by the legislature; and it requires information regarding the exercise of such powers to be collated in a publicly available document.

9.63 The Commission recognised that the advantages of transparency and having the powers collated for research purposes must be balanced against the administrative burden that such reporting requirements impose.[48] It thought that annual reporting was justified for warrantless searches because they are not subject to the same external scrutiny as powers exercised under warrant; and for surveillance device warrants because they are almost always exercised covertly, which increases the need for accountability and transparency.[49]

9.64 In relation to production orders, one of the main reasons for annual reporting would be to assess whether the power is being used appropriately. Some questions in relation to production orders that may be of public interest might include:

---

44 Search and Surveillance Act 2012, s 172.

45 Section 170(1)(c).

46 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [4.45]. We note that the Commission's recommendation was in relation to "residual warrants", which were changed to "declaratory orders" during the legislative process. Similarly, examination orders were not discussed in the Commission's Report.

47 At [15.45].

48 At [15.46].

49 At [15.47]–[15.48]. The Commission did not discuss whether there should be a reporting requirement in relation to production orders in its Report.

- Are the numbers of production orders that are applied for increasing or decreasing over time and if so, why is that?
- To what extent and in relation to what type of information and what type of organisations are enforcement agencies obtaining information by voluntary disclosure rather than by production orders?
- Are there regional differences in the number or nature of production orders?
- Are production orders placing an unreasonable burden on some entities?[50]

9.65 Annual reporting of simply the number of production orders applied for would only be relevant to the question of the increase or decrease in numbers over time. It would not provide information as to the cause of that trend. Other information that might elucidate that trend or answer the other questions would include:

- the nature of the offences in relation to which production orders were applied for;
- the type of information sought under production orders;
- the number of requests for voluntary disclosure of information (and the type of information sought); and
- a regional breakdown of the information above.

9.66 The issue for this review is whether there is sufficient benefit to be gained from requiring enforcement agencies to report on production orders to justify the cost to those agencies in gathering the statistics. It is possible that the benefit will only be gained if the requirement covers some other details beyond the bare number of production orders applied for each year. If so, that increase in benefit must again be weighed against the increase in compliance costs. We note that, given the high number of production orders applied for each year and the even higher number of requests for voluntary disclosure of information, there could be a significant compliance burden associated with such a reporting requirement.

9.67 The international trend towards transparency reporting described above indicates that some organisations that are commonly subject to government requests for data are

---

[50] We note that companies approached to participate in the Privacy Commissioner's trial of transparency reporting said that on average it took half an hour to process a typical request. That figure is the average for all types of requests for information, and is likely to differ significantly depending on the nature and quantity of the information requested. See Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 8.

interested in greater transparency around this sort of activity. That interest appears to stem from a perception that their customers are concerned about:[51]

- whether their personal information is kept private;
- how their information is accessed and used by the government; and
- whether the trade-off of privacy for law enforcement is proportionate.

9.68 We note that in the Privacy Commissioner's report, some of the companies approached to participate in the trial expressed frustration that government agencies did not themselves report on the number of requests for information they made.[52]

9.69 However, we also note that:

- It would perhaps be strange if enforcement agencies were required to report on production orders but not on search warrants, given that production orders were introduced as a less intrusive alternative to search warrants.
- A requirement to report on production orders may provide an unintended incentive for agencies to use other mechanisms to obtain information, such as voluntary disclosure. That risk would, of course, be mitigated if the Act was amended to be clearer about when a production order is required or to require reporting of requests for voluntary disclosure.

Q42 Should enforcement agencies be required to report annually on the number of production orders they have applied for and the outcome of those applications?

NOTICE REQUIREMENTS

9.70 There is a question for this review about whether the people whose information is disclosed by a third party to an enforcement agency under a production order should be given notice of that disclosure. We note that this issue may apply equally to search warrants.[53] There are two opposing views here. The first view, from a privacy perspective, suggests that the Act should specifically permit the third party to inform their customer of the production order or, alternatively, require the enforcement

---

51 Privacy Commissioner *Transparency Reporting Trial*, above n 15, at 6–7.

52 At 11.

53 As we discuss below at paragraph [9.78], the Act requires a person exercising a search power to provide a copy of the search warrant to the occupier of the place to be searched (or person in charge of the vehicle or other thing to be searched) and an inventory of the items that were seized (ss 131(1) and 133); however, the occupier may not be the person whose items are seized.

agency to inform the person. Under this view, the person whose information is disclosed has a right to know that their information has been accessed so that they can defend their rights if necessary.

9.71 This issue was raised in 2010 when the Search and Surveillance Bill was before the Select Committee. In her submission to the Committee, the (then) Privacy Commissioner argued that enforcement officers should be required to notify the person whose information was obtained that an order was made and the details of the information that was produced. The Committee rejected the idea on the basis that there is no comparable obligation when information is gathered from third parties under a search warrant.[54]

9.72 The second view, from a law enforcement perspective, suggests that the Act should be clearer that the third party must *not* inform the person whose information is disclosed, as that disclosure may prejudice the ongoing criminal investigation.

Current law

9.73 During our preliminary consultation, it was suggested to us by one agency that the Act already makes it an offence for a third party to disclose the fact of a production order to its customer. Section 179 states:

> (1) No person who, as a consequence of any thing specified in subsection (2), acquires information about any person may knowingly disclose the substance, meaning, or purport of that information, or any part of that information, otherwise than in the performance of that person's duties, functions, or powers.
>
> (2) The things referred to in subsection (1) are—
>
> (a) the exercise of a search or surveillance power:
>
> (b) an examination order:
>
> (c) a production order:
>
> (d) the use of a device, technique, or procedure, or the carrying out of an activity specified in a declaratory order.

9.74 Under a literal interpretation, a third party who discloses the existence of a production order may breach this provision. The "purport" of a production order is that the person whose information is sought is under investigation. By communicating the fact of the production order to that person, the third party would be disclosing that purport (which they acquired as a consequence of the production order) to that person. However, there

---

[54] Search and Surveillance Bill 2010 (45-2) (select committee report) at 12.

are indications that this provision was intended to apply only to enforcement officers and other people within enforcement agencies who acquire the information.

9.75 When the Search and Surveillance Bill (that was ultimately enacted) was introduced in 2009, this provision read:[55]

> No person who, *as a consequence of exercising a search or surveillance power* or as a consequence of assisting another person to exercise a power or carry out an activity of that kind, acquires information about any person may knowingly disclose the substance, meaning, or purport of that information, or any part of that information, otherwise than in the performance of that person's duty.

9.76 The Law Commission and the Ministry of Justice pointed out in their departmental report on the Bill that the clause, as drafted, was limited to people who acquire information when they themselves exercise a search or surveillance power.[56] They considered it should extend to "other people who may have access to such information (eg, a computer technician)".[57] Accordingly, they recommended that the clause be amended so that it is an offence *for anyone to disclose information that is acquired through the exercise of* a search power, surveillance power, an examination order, a production order, or activities carried out under a declaratory order.[58]

9.77 The clause in the Bill was amended accordingly, but the new wording omitted the words "the exercise of", which makes it unclear whether it was intended to extend beyond members of the enforcement agency.

Other notification requirements in the Act

9.78 There are a variety of other notification requirements in the Act. A person exercising a search power must announce their intention to search and provide the occupier of the place searched (or person in charge of the vehicle or thing searched) with a copy of the search warrant and a list of the things that were seized.[59] However, if the information sought relates to a person who is not the occupier, there is no corresponding obligation to notify that other person of the search. If the occupier of the place searched is not

---

55 Search and Surveillance Bill 2009 (45-1), cl 171 (emphasis added).

56 Ministry of Justice and Law Commission *Departmental Report for the Justice and Electoral Committee* (August 2010) at [612].

57 At [612].

58 At [614].

59 Search and Surveillance Act 2012, ss 131(1) and 133.

present at the time of the search, written notice of the search and things seized must be left at the place.[60] A judge may defer those obligations to provide notice for up to 12 months if providing notice would endanger the safety of a person or prejudice ongoing investigations.[61]

9.79 A person who conducts a remote access search must send an electronic message to the email address of the thing searched, attaching the warrant and setting out particulars of the search.[62] It is only if that message is unable to be delivered that the person conducting the search has an obligation to take all reasonable steps to identify and notify the user of the thing searched.[63] As we discuss in Chapter 6, there is currently no power to defer notice of a remote access search.[64]

Analysis

9.80 The main advantage of requiring notice to the person whose information is sought under a production order is that it increases transparency and allows the individual to challenge the disclosure if there are grounds to do so. In theory, it may also allow a person to claim any relevant privilege in respect of the information, although we note that notice would probably occur after the production order is executed, rather than before, so any privileged material may have already been seen.

9.81 Conversely, the main disadvantage of notification is that it may prejudice the future law enforcement investigation. This risk is perhaps greater for production orders than for search warrants because they tend to be used at an earlier point in an investigation. For example, if the individual is informed that his or her text messages have been disclosed under a production order, he or she may take steps to hide evidence that might otherwise be found in the execution of a subsequent search warrant. This risk could be mitigated by allowing deferred notification as is permitted under section 134.

9.82 If the Act required the enforcement agency to provide notification, it could be quite time-consuming to identify and notify each of the people for whom information is sought. Delayed notification is likely to be required frequently. In general, we note

---

60 Search and Surveillance Act 2012, s 131(4).

61 Section 134. This power is generally used in relation to covert operations.

62 Section 132(1).

63 Section 132(2).

64 See paragraph [6.109] above.

that it may be more efficient for the third party to provide notification, particularly if they maintain a database of contact information.

Q43 Should the Act require or enable notification to a person whose information is disclosed under a production order?

Q44 If you do not favour notification, should the Act prohibit third parties from disclosing the fact of a production order to the person whose information is sought?

PRESERVATION ORDERS

9.83 Unlike equivalent legislation in most of the other jurisdictions we compare ourselves to, the Act does not provide a regime under which entities that hold information relevant to criminal investigations can be required to temporarily preserve that information while a search warrant or production order is sought. The type of information often required for law enforcement purposes may not be retained for the business purposes of the network operator. It may be deleted or over-written within days after its creation. Two common examples are telecommunications information (either the content of the communications or the metadata associated with it) and footage from CCTV surveillance. An issue for this review is whether the Act should provide a mechanism for requiring temporary preservation of specified information relating to an investigation while an enforcement officer seeks authorisation to access it.

9.84 Preservation of data is often confused with the retention of data. Preservation refers to a requirement to preserve and maintain the integrity of certain *particularised data* for a temporary period while the enforcement agency seeks authorisation to access it. Retention refers to a requirement to retain certain *types of data* for a fixed period of time so that it may be available if the enforcement agency considers it is necessary for an investigation. Both types of regimes provide merely for the capturing of data. Enforcement agencies must then rely on whatever regime is applicable to access the information, such as a search warrant or production order.

9.85 Currently, the Act does not provide for the preservation of data. A production order only requires a third party to provide documents in their possession or control as at the date of the production order. Any documents deleted or lost before that date are not available for law enforcement purposes.

Possible problems

Access to potential evidence

9.86 The information sought under a production order is usually personal information stored by a third party service provider. The collection, storage and use of that personal information is governed by the Privacy Act 1993. Information privacy principle nine under that Act limits the timeframe within which personal information can be stored:[65]

> An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

9.87 This means that companies can only keep their customers' personal information for the time it is relevant to their business purposes. They may also frequently over-write data due to limited storage capacity. That may be a shorter period than is required for law enforcement purposes. In practice, some data is deleted within hours or days of its creation, but it may take several days to obtain a production order. By the time a production order comes into force, the relevant information may no longer be stored. While there is provision in the Act to make oral applications for production orders,[66] that procedure is designed for exceptional circumstances only.

9.88 We would be interested to hear feedback on the extent of this problem and how it is being influenced by the changing nature of our use of telecommunications and the changing nature of the industry.

Budapest Convention

9.89 The absence of a regime in the Act for preserving computer data for law enforcement purposes is one of the key reasons New Zealand has not yet acceded to the Budapest Convention,[67] which we described in Chapter 6. Article 16 of the Convention requires States to adopt legislative or other measures to enable law enforcement agencies to order the expeditious preservation for up to 90 days of computer data that is vulnerable to loss or modification. Although a preservation regime in the Act could apply more

---

65 Privacy Act 1993, s 6, principle 9.

66 Search and Surveillance Act 2012, s 100(3).

67 Council of Europe Convention on Cybercrime ETS 185 (opened for signature 23 November 2001, entered into force 1 July 2004) [Budapest Convention].

broadly than to computer data, it would seem that such a regime would remove a key hurdle to New Zealand's accession to the Convention.

9.90 The Government has said that it will consider progressing New Zealand's accession of the Budapest Convention as part of its 2015 cybercrime strategy.[68] The advantages of acceding to this Convention are three-fold:

- it would enhance New Zealand's reputation as a trusted international partner;
- it would provide a platform to enable an expansion of reciprocity arrangements with foreign law enforcement agencies; and
- it would strengthen New Zealand's ability to fight transnational crime.

9.91 These three advantages are inter-related and are demonstrated by way of the example of cross-border searches of digital material. As we described in Chapter 6, often digital material accessed via the Internet is stored on a server located overseas.[69] The only official way to access information located in another jurisdiction is through a process of mutual legal assistance. That process can take months, which is obviously an impediment to the effective investigation and prosecution of crime.

9.92 We also described in that chapter how other jurisdictions have begun negotiations to provide a solution to this problem. The negotiations are aimed at agreeing on new international treaties that would allow law enforcement agencies from one State to issue warrants or orders to communications companies in other States, requiring them to provide access to information for the purposes of investigating crime.[70] The key negotiating hurdle for these treaties is assurance that the powers to issue warrants and orders are subject to adequate protections for the privacy of personal information.

9.93 It is in New Zealand's interests to be party to these negotiations – both from a law enforcement perspective (it would provide more efficient access to data for investigations) and from a privacy perspective (it would provide more assurance that requests for information are subject to strict controls). However, our accession to the Budapest Convention is seen as a key prerequisite to enter these negotiations because

---

68 Department of Prime Minister and Cabinet "New Zealand's Cyber Security Strategy" (December 2015) <www.dpmc.govt.nz/dpmc/publications/nzcss>. See *National Plan to Address Cybercrime* (2015) at 14.

69 See paragraph [6.113] above.

70 Ellen Nakashima and Andrea Peterson "The British Want to Come to America – With Wiretap Orders and Search Warrants" *The Washington Post* (online ed, Washington DC, 4 February 2016).

it would demonstrate that our laws have reached the standard required by that Convention.

Overseas jurisdictions

Canada

9.94 Canada recently included a preservation regime in its Criminal Code, which enabled it to accede to the Budapest Convention in July 2015. The regime provides for preservation demands and preservation orders, which can apply to any type of computer data.

9.95 A preservation demand may be made by a peace officer or a public officer and requires the specified data to be preserved for 21 days.[71] The enforcement officer making the preservation demand may impose conditions in the demand, including a prohibition on disclosing the existence of the demand or its contents. A preservation order is made by a justice or judge on application by a peace officer or public officer.[72] It requires the specified data to be preserved for 90 days.

Australia

9.96 Australia acceded to the Convention in November 2012. The Cybercrime Legislation Amendment Act 2012 was passed for the purpose of implementing that Convention. It provides a preservation regime in respect of telecommunications data only. Under that regime, a law enforcement agency may give a preservation notice to a telecommunications provider that is in force for 90 days.[73] We have heard that preservation notices have never been used in Australia. If that is correct, it is likely to be because telecommunications providers in that country are also subject to requirements to retain certain metadata for two years.[74]

---

71 Criminal Code RSC 1985 c C-46, s 487.012. The Code defines "peace officer" and "public officer" as including a wide range of people, such as mayors, sheriffs, members of the Correctional Service, police officers and bailiffs.

72 Criminal Code RSC 1985 c C-46, s 487.013. If the offence in question was committed in a foreign State, the justice or judge must also be satisfied that a person or authority with responsibility in that State for the investigation of such offences is conducting the investigation.

73 Telecommunications (Interception and Access) Act 1979 (Cth), ss 107H–107K (as amended by the Cybercrime Legislation Amendment Act 2012 (Cth)).

74 Telecommunications (Interception and Access) Act 1979 (Cth), s 187C.

United Kingdom

9.97 The United Kingdom signed the Convention in 2001 and ratified it in May 2011. It does not have a regime for preservation orders in its domestic legislation because it has a data retention regime instead. Under the Data Retention and Investigatory Powers Act 2014 (UK) (DRIPA), telecommunications operators can be required to retain communications data for up to 12 months. In November 2015, the United Kingdom Government introduced the Investigatory Powers Bill, designed to consolidate the powers in DRIPA and two other statutes regulating telecommunications. That Bill is currently under consideration by the House of Lords.

Options for reform

9.98 The Act could be amended to include a preservation regime if the deletion of data in the ordinary course of business is impeding effective law enforcement, or if New Zealand wishes to accede to the Budapest Convention. We wish to hear submitters' views on whether the current inability to require preservation of data has been causing problems in practice.

9.99 There are a number of options for framing the scope of a preservation regime. To date, we have done little analysis of the implications of these various options. We mention them here to seek feedback and to give a sense of the questions that would need to be resolved.

Type of data holder

9.100 There are a variety of options for defining who may be subject to a preservation request. It could be as broad as a production order – "any person" could be requested to retain information.

9.101 Alternatively, it could follow the Australian model and be confined to telecommunications providers on the basis that telecommunications data is particularly vulnerable to deletion or modification. Within the telecommunications industry, it could be limited to retail providers because they hold the vast bulk of relevant data and wholesalers are merely the conduit for communications to the retail sector. Telecommunications data is of special interest because of its unique value for the investigation of offences, the fact that searches of it can be highly intrusive of privacy and because compliance with any preservation regime would presumably require significant investment and infrastructure on the part of telecommunications providers.

9.102 Any proposal for a preservation regime would need to have considered the compliance costs for the relevant data holders.

Types of data

9.103 A preservation regime could either define the type of data that may be subject to a preservation request or it could build that into the threshold test. For example, the provision could state that a request to preserve data may only be made if the person making the request has reasonable grounds to believe that the data will be lost before an application for a warrant or production order can be determined.

9.104 In respect of telecommunications data, it is likely that a preservation regime would need to include both content and metadata.

9.105 Additionally, any preservation regime should be clear that the requirement is only to preserve documents that are already stored in the normal course of business. An obligation to store a certain type of data in case it is required in the future is, in effect, a retention regime.[75] This is not required under the Budapest Convention and is not being considered in this review.

9.106 It is noted that, while the obligation to preserve documents would only apply in respect of data already stored in the normal course of business, it is likely that some businesses would need to adapt their systems to enable them to extract and store the specific data requested for the duration of the order.

Issuing entity

9.107 The two options for who might have authority to issue a preservation request appear to be either the enforcement agency that wishes the data to be preserved or an issuing officer under the Act. We note that the Australian legislation permits the law enforcement agency to issue a preservation notice.[76] However, as mentioned, the Canadian legislation has separate regimes for:[77]

- a "preservation demand" issued by a peace officer or public officer for only 21 days; and

---

[75] We described the difference between a preservation regime and a retention regime above at paragraph [9.84].

[76] Telecommunications (Interception and Access) Act 1979 (Cth), s 107H (as amended by the Cybercrime Legislation Amendment Act 2012 (Cth)).

[77] Criminal Code RSC 1985 c C-46, ss 487.012 and 487.013.

- a "preservation order" issued by a justice or a judge for 90 days.

9.108 We can immediately see two disadvantages to requiring preservation orders to be made by issuing officers. First, if the purpose of a preservation regime is to ensure that data is not lost while a production order or search warrant is applied for, it would seem to defeat that purpose to require an application to be made to an issuing officer. Any such application is likely to take almost as long as applying for a production order. Second, given that preservation does not authorise an agency to access the data (it merely preserves it), there may be insufficient justification to impose this administrative burden and extra cost on both enforcement agencies and the court system.

Threshold for a preservation request

9.109 The Budapest Convention does not address the appropriate threshold for issuing a preservation order, although it states that the requirement for a preservation regime is particularly relevant "where there are grounds to believe the computer data is particularly vulnerable to loss or modification".[78] There are a variety of options for framing this threshold. One option is for the threshold to be the same as for a production order, meaning that there must be:

- reasonable grounds to suspect that a relevant offence has been, is being, or will be committed; and
- reasonable grounds to believe that the documents specified will constitute evidential material in respect of that offence and will be in the possession or control of the person subject to the request at the time it is made.

9.110 This may be considered to be appropriate if the purpose of preservation orders is to ensure that the data is not deleted while the enforcement agency applies for a search warrant or a production order.

9.111 However, it may be thought that a slightly lower threshold is appropriate, given the enforcement agency may need more time to gather all the evidence required to meet the grounds for a production order or search warrant. We note that the Canadian threshold for a preservation demand or preservation order only requires "reasonable grounds to suspect" that the computer data is in the person's possession or control,

---

[78] Budapest Convention, above n 67, art 16.1.

rather than "reasonable grounds to believe" as is required for a search warrant in New Zealand.[79] Also, the Canadian thresholds only require the computer data to "assist in the investigation of the offence", rather than "constitute evidential material", as is required in New Zealand. Similarly, the Australian thresholds only require "reasonable grounds to suspect" that the data exists and "might assist in connection with the investigation".[80]

Duration of preservation

9.112 The Budapest Convention requires that any preservation regime provides for computer data to be preserved for up to 90 days. As already mentioned, the Australian and Canadian regimes also provide for preservation notices to be in force for 90 days (or in Canada, for only 21 days if the demand is made by the enforcement agency).[81] Subject to feedback from enforcement agencies as to the adequacy of that time period for law enforcement purposes, we doubt there would be reasons to extend the requirement beyond the time period set out in the Convention.

Prospective preservation requests

9.113 Currently, a production order may require a person to either produce a document on one occasion or to produce a type of document on an ongoing basis for the duration of the order.[82] A preservation regime could similarly target either documents already in the possession or control of the person (retrospective preservation) or any documents that will come into the person's possession or control (prospective preservation). In either case, the data would be held for up to 90 days or for whatever maximum period is specified in the Act.

9.114 The Budapest Convention does not require prospective preservation but the Australian legislation provides for it, nonetheless.[83] The main advantage of allowing for

---

79 Criminal Code RSC 1985 c C-46, ss 487.012(2)(c) and 487.013(2)(a). We note that there is an additional condition relevant only when the offence is committed under a law of a foreign State. Also, when a justice or judge is making the determination, he or she must also be satisfied that a peace officer or public officer intends to apply or has applied for a warrant or an order in connection with the investigation to obtain a document that contains the computer data.

80 Telecommunications (Interception and Access) Act 1979 (Cth), s 107J.

81 Telecommunications (Interception and Access) Act 1979 (Cth), s 107K; Criminal Code RSC 1985 c C-46, ss 487.012 and 487.013.

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

83 Telecommunications (Interception and Access) Act 1979 (Cth), s 107H(1)(b)(ii).

prospective preservation (besides the advantage of aligning with the production order regime) is likely to be that it avoids the need for enforcement officers to make multiple preservation requests (or apply for multiple preservation orders).

9.115 If requests for prospective preservation were permitted, the Act would need to specify the time period in which that request applied. We note that production orders can be in force for 30 days. It may be that a similar time period is appropriate.

Q45 Is there a problem with data being unavailable by the time enforcement agencies have obtained a search warrant or production order?

Q46 Should the Act be amended to include a preservation regime? If so, do you have views on the design of that scheme?