Transparency Reporting Summary Report

October 2017

Executive Summary

Transparency about what happens to people's information is an important part of upholding privacy rights. Transparency reporting promotes good privacy practice, with benefits to both individuals and agencies. This is particularly relevant today, when the amount of information collected about individuals is increasing. The practice of transparency reporting is developing, with new guides and templates now widely available.

Law enforcement agencies must account for, and be transparent about, their use of intrusive powers to ask agencies for the personal information they hold. Agencies who seek to rely on Privacy Act exceptions to request disclosure of personal information from others must make clear, specific, requests and demonstrate that the disclosure is necessary.

Our Office has developed guidance for agencies making requests for disclosure of information under principle 11(e)(i) and (f) of the Privacy Act.

Introduction

1. We live in an increasingly data rich world. Data about people – what they like, where they go, who they are friends with – has huge potential value for commercial companies and government agencies alike. Allowing data to be used in this way has value for individuals, such as being offered customised products and services. But there are also risks; data breaches, discriminatory profiling or inappropriate disclosure of personal information can all cause real harm. Good privacy and security protections are essential.

2. Law enforcement and intelligence and security agencies have a particular interest in company-held information. Cell phone providers, utilities and banks, for example, hold information that can reveal a customer's movements, contacts and financial transactions.

3. Transparency about what happens to people's information is an important part of upholding privacy rights. Transparency helps ensure accountability. It allays suspicions by allowing people to see what really happens, and doesn't happen, with their information. Being transparent with their customers about how their information is being used is the *quid pro quo* for companies being able to hold and use data for commercial gain.

4. This Office has a strong interest in promoting transparency reporting by New Zealand companies. This report discusses the work we have done over the last two years, developments here and overseas related to transparency reporting, and introduces a range of resources that are now available to companies, including guidance we are publishing alongside this report.

What is transparency reporting?

5. ‘Transparency reporting’ is public reporting by companies that hold personal information about the information requested by and disclosed to government agencies, usually for law enforcement or national security purposes. The content of transparency reporting may differ between different companies and jurisdictions but the aim is usually the same; to be transparent about what happens with personal information in order to promote accountability and to maintain customers’ trust.

6. There are significant benefits for individual privacy from transparency reporting, including:

   - prompting agencies to ensure that the use of their coercive powers is proportionate and justifiable;

   - giving consumers insight into the actions of companies regarding the use, protection and disclosure of the personal information they hold; and

   - encouraging companies to adopt good processes for handling requests.

7. Transparency reporting can also allay suspicions by providing real data, rather than speculation about the extent of access by law enforcement agencies. For example, there was significant public concern about the extent of company cooperation with intelligence and security agencies following the 2013 disclosures related to the extent of government surveillance of global online activity. Transparency reporting is a useful counter measure to such a climate of distrust.

OPC transparency reporting trials

8. Given the potential benefits of transparency reporting, in 2015 we began a project to see if there was a role the Office of the Privacy Commissioner could play in promoting and supporting more New Zealand companies to publish their own transparency reports.

9. Our objective was to understand the benefits of, and impediments to, companies engaging in transparency reporting. Internationally there is a growing momentum for transparency reporting and we would like to see more companies engaging in transparency reporting in New Zealand.

10. As part of that work we recruited approximately a dozen companies from the financial services, utilities and telecommunications sectors to collect data on the number of requests for customer information they received from law enforcement agencies. These companies provided this data to us, and we aggregated it and published a report on the findings.

11. You can find the report from our August-October 2015 trial here and from the April-June 2016 trial here.

12. The Privacy Act presumption is that agencies will not disclose personal information to other agencies. The Act then sets out a range of exceptions whereby information can be disclosed. For example, principle 11(e)(i) allows information to be disclosed where necessary to avoid a prejudice to the maintenance of the law. There are also other statutes that override the Privacy Act that allow law enforcement and regulatory agencies to collect personal information in certain circumstances.

13. The results from the two trials showed law enforcement agencies make thousands of requests for personal information from companies every month.

14. Most requests came from Inland Revenue, the Ministry of Social Development, and the Police. The most commonly used legal grounds for collection of information were section 17 of the Tax Administration Act, section 11 of the Social Security Act, voluntary disclosure of information under one of the exceptions to principle 11 of the Privacy Act, followed by production orders under the Search and Surveillance Act.

15. There was significant media interest in the results of our trials. This is indicative of a high level of public interest in how law enforcement agencies are using their information gathering powers, and how companies and treating personal information.

Domestic and international developments

16. Since we began this work, there have been several high profile cases involving law enforcement requests for personal information. In New Zealand, the case of Westpac Bank's disclosure of Nicky Hager's information to the Police has highlighted the public interest in such information requests. Internationally, data protection and privacy commissioners have stated their support for transparency reporting, and more resources are available to support companies to begin transparency reporting.

Hager / Westpac

17. The high levels of interest into the Commissioner's investigation into Westpac bank disclosing journalist Nicky Hager's bank account information to Police in 2014 indicates that transparency is a live issue for the public and media. The general public want to know when agencies that hold personal information share this with law enforcement agencies and what controls there are on these disclosures.

18. As part of a Police investigation into offences under section 249 of the Crimes Act (accessing a computer for a dishonest purpose) and fraud, Police asked Westpac Bank for information about Mr Hager. Mr Hager was not a suspect in the criminal investigation. Westpac provided Police with several months of Mr Hager's transaction information. The Police did not use a production order to request this information.

19. In releasing this information to Police, Westpac relied on individual authorisation (principle 11(d) of the Privacy Act) because the bank's terms and conditions included a clause that Westpac would disclose information to Police whenever it "reasonably believes that the disclosure will assist it to comply with any law, rules and regulations in New Zealand or overseas or will assist in the investigation, detection and/or prevention of fraud, money laundering or other criminal offences."

20. Mr Hager had accepted the terms and conditions and Westpac believed that provided sufficient grounds to respond positively to the Police request for information. During our investigation we also considered the application of privacy principle 11(e)(i), which allows disclosure to avoid prejudice to the maintenance of the law.

21. We found that the wording of the Westpac terms and conditions meant that its customers would reasonably believe the kinds of criminal offences where information might be disclosed would more likely be limited to financial crimes. The Commissioner's view was that Westpac had interpreted the wording "other criminal offences" in its terms and conditions too broadly. We did not support the argument that the wording included a broader "necessary to avoid prejudice to the maintenance of the law" meaning. Police had not offered any reasons why the information was required for the maintenance of the law and Westpac could not logically rely on the concept of customer authorisation and the maintenance of the law exception concurrently.

22. Since the Westpac / Hager case, we have seen encouraging signs of agencies taking steps to improve their processes for making and receiving requests for information. For example, the Police have revised their standard information request form to improve the consistency of practice by Police officers. Agencies, including banks, have also approached this Office for advice on how they should handle requests for information made without compulsion. It is in part in response to such requests that we are now publishing the guidance that accompanies this report.

23. In early 2017, the Bankers' Association signed a letter of agreement with the New Zealand Police on behalf of its members.[1] The letter describes how the Fraud Group of the New Zealand Bankers' Association and the Police will work together on their common goal of reducing crime and increasing community safety within the banking environment. Among other things, the letter formalises how the Bankers' Association and the Police will work together to develop policies and procedures for operational matters, such as requests for information.

Complaints received by the Office of the Privacy Commissioner

24. Complaints received by the Privacy Commissioner under the Privacy Act underscore the need for companies to be open with customers about what happens with their data.

[1] http://www.nzba.org.nz/consumer-information/fraud-protection/reducing-crime-with-the-nz-police/

25. For example, a journalist has written about his experience of trying to get his cell phone provider to tell him whether any law enforcement agencies had made requests for information about him.[2] The company's initial response was to 'neither confirm nor deny' whether any law enforcement agencies had made requests for information about his account.

26. Mr Marwick complained to the Privacy Commissioner about not being able to get access to his personal information. The Commissioner considered the company's actions, and concluded that they were in the wrong for taking a blanket 'neither confirm nor deny' approach to all such requests for information. The Commissioner's view was that an individual's right to access information about themselves includes information about who has viewed their data, and that companies have to consider each request on a case by case basis.

Resolution on transparency reporting by 37th International Conference of Data Protection and Privacy Commissioners

27. The 57th meeting of the International Working Group on Data Protection in Telecommunications in Seoul, 27-28 April 2015 adopted a Working Paper *"Transparency Reporting: Promoting accountability when governments access personal data held by companies".* The argument set out in the paper is that transparency reporting has value in promoting trust in organisations with substantial holdings of personal data, and holding public authorities accountable where they seek access to that data.

28. The working paper noted that government demand for access to personal information held by companies has grown in scope since 2011. Since then, high profile terrorism incidents have enabled security and law enforcement concerns to prevail over traditional norms of company confidentiality. At the same time, technological advancements (including reduced data storage costs, previously specialised analytical techniques becoming mainstream, cloud service providers and increased volumes of data) have increased the attractiveness for governments of accessing company-held personal information.

29. In contrast to the traditional search warrant, the emergence of production orders has shifted the administrative burden of locating, assembling and producing documents for government inspection onto companies. The paper also noted a trend of governments requiring companies to keep documents for extended periods, beyond any business need, in case the information may be useful to law enforcement authorities in the future.

30. The frequency of requests and the volumes of information passing from companies to government agencies is unclear. The working paper called for greater accountability and transparency around both the requesting and responding agencies' actions. The paper recommended that companies develop clear company policies for handling government requests, including standardisation, criteria aligned with legal requirements and the involvement of senior staff, to ensure the requests are handled appropriately and to avoid mistakes.

[2] http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11629635

31. The paper sets out some of the benefits of transparency reporting, including that greater reporting would illustrate that privacy is important to the company concerned, would have reputational benefits, would promote the accountability of public agencies and ensure that they take care to use their coercive powers in proportionate and justifiable ways. The working paper suggested that transparency reporting should be underpinned by the following principles: accountability, transparency, reliability, truthfulness, comparability and accessibility.

32. Transparency reporting would also enable statistical analysis on the number and nature of government requests for company information, and the outcome of those requests. Over time, it would enable analysis of trends and the factors leading to greater or reduced demand for company data.

33. Following on from the Working Paper, and its recommendations, Data Protection and Privacy Commissioners from around the world passed a Resolution on Transparency Reporting at their 37th International Conference on 27 October 2015 in Amsterdam.

34. In this resolution the Data Protection and Privacy Commissioners urged governments to:

- keep records on the number, nature and purpose of lawful access requests for information held by organisations;

- develop consistent reporting across jurisdictions, explaining how often requests for personal data are made, and for what purposes, with goal of regularly publishing such records; and

- remove legal or administrative barriers to transparency reporting.

35. The resolution also urged organisations to:

- conduct rigorous due diligence prior to responding to government requests for personal information to ensure the lawful basis of such requests and to maintain consistent records for reporting;

- document and explain to the public and supervisory authorities their internal policies and procedures for dealing with security and law enforcement requests;

- publish reports on the number of requests made, nature of responses and legal basis for government access to the personal information requested.

36. Lastly, the resolution urged data protection authorities, oversight bodies and review agencies involved in supervision of surveillance activities to ensure trustworthy, independent and publicly accountable oversight where they can.

Resources for companies

37. Good resources are now available to support companies to produce simple and comparable reports. For example, in mid 2015 the Canadian Government published transparency reporting guidelines for private sector companies. The purpose of the guidelines is to "help private organizations be open with their customers, regarding the management and sharing of their personal information with government, while respecting the work of law enforcement, national security agencies, and regulatory authorities."[3]

38. The Guidelines provide companies with the following categories of disclosures to report against:

- voluntary disclosures at the request of a government organisation
- voluntary disclosures on the initiative of the organisation
- disclosures in emergency or exigent circumstances
- disclosures made in compliance with federal or provincial law
- court ordered (warranted) disclosures
- other.

39. For each category, the guidelines advise companies that they could report statistics such as the number of requests received from government authorities, the number of requests fulfilled, the number of requests rejected or contested, and the number of persons or accounts whose information was disclosed.

40. The guidelines also provide advice on limitations to consider when reporting statistics, to minimise the risk of compromising national security or criminal investigations. For example, the recommend that figures between 0 and 100 should be represented in a band of '0-100', figures should not be broken down by region or specific agency, and reporting should be delayed by at least 6 months.

41. In 2016, Internet NZ, an organisation which promotes a safe and open internet in New Zealand, launched a set of 'easy transparency' tools for Internet Service Providers (ISPs).[4] The tools include a template policy and report, and spreadsheet for collecting data. Whether or not an ISP publishes its own transparency reports is one of the criteria on Internet NZ's ISP scorecard.[5]

[3] http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html
[4] https://internetnz.nz/easy-transparency
[5] https://internetnz.nz/ispreview

42. Internationally, Harvard University's Berkman Klein Centre for Internet & Society have published a transparency reporting guide and toolkit to encourage more companies that receive requests for information from American government agencies to undertake transparency reporting.[6] The guide highlights best practice by companies that are already producing regular transparency reports and seeks to make it easy for new companies to start reporting.

43. TradeMe has led the way in New Zealand, publishing transparency reports each year since 2013. TradeMe's rationale for transparency reporting is stated in its 2017 report as: "Being 'honest and straight up' is enshrined in our company values, and we think this report helps our community understand our approach to privacy."[7] TradeMe notes in its 2017 report that it regularly gets approached for advice by other businesses interested in transparency reporting. As yet, it appears that TradeMe is still the only New Zealand company to publish such reports, but it is encouraging to note that others are at least actively considering it.

44. By publishing this report, and the guidance that accompanies it, we hope to encourage companies to begin to publish their own transparency reports, using the resources now available.

Intelligence and Security agencies

45. Transparency reporting has its roots in US companies' concerns about surveillance by security and intelligence agencies. Concern about surveillance is also evident in this country; in a 2014 survey carried out by this office, 34% of respondents were 'very concerned' about surveillance of New Zealanders by the Government.

46. We excluded requests for information from the GCSB and SIS out of our 2015 and 2016 transparency reporting trials. The GCSB and SIS have extraordinary powers due to the exceptional nature of their work, and at the time of the trials, the legislation governing these agencies was under review. While we therefore elected to leave the security and intelligence agencies out of our trials, this does not mean that we think that reporting about the information gathering activities of these agencies is not important. There was some ambiguity at the time about the intelligence and security agencies' authority to participate in the trials. Their legal situation at the time was more opaque than we would have liked as their collection was governed by different classified instruments.

47. The review of the intelligence and security legislation partly reflected a need for greater transparency about, and greater public trust and confidence in, the activities of these agencies. In early 2017, Parliament passed a new Intelligence and Security Act. This Act increases the application of the Privacy Act to the security and intelligence agencies. It also adds a new exception to principle 11, to allow agencies to disclose information to the security and intelligence agencies where necessary for them to fulfil their functions under certain parts of the Intelligence and Security Act.

[6] https://cyber.harvard.edu/node/99763
[7] http://www.trademe.co.nz/trust-safety/transparency-report-2017/

48. The new exception means that the legislation governing the security and intelligence agencies now more closely resembles the regime for other law enforcement agencies. This should enable statistics about the requests for information made by these agencies to be more easily reported by companies.

49. The Intelligence and Security Act 2017 also includes specific procedures for accessing records held by telecommunications agencies (Part 5, subpart 4). The Act allows the security and intelligence agencies to acquire personal information by compulsion, but only for specific types of information (content is excluded), subject to procedural safeguards.[8]

Reporting by government agencies

50. Several companies suggested to us that data on the use of law enforcement agencies' information gathering powers would be better produced by the agencies themselves. We agree; to some extent, transparency reporting is a response to a gap left by a lack of reporting by government agencies.

51. Some agencies, including Police and the security and intelligence agencies, are subject to statutory requirements to report on the use of certain search and surveillance powers. However, the vast majority of information requests go unreported. We think that ideally law enforcement agencies should be monitoring, auditing, and reporting on the use of the information gathering powers. However, in the absence of such reporting, transparency reporting provides important information for the public.

Conclusions

52. Over the last two years we have seen encouraging signs that companies see value in transparency reporting. However, most are still reticent about investing in producing their own reports.

53. From conversations with companies through our 2015 and 2016 transparency reporting trials, it seems that the primary barrier to companies engaging in transparency reporting is operational. Of the companies we spoke to, for those that have a single person or team that receives and processes requests for information, collecting data on the number and type of requests was relatively simple. However, for companies where requests could come into any number of business units or branches, significant time and resources were needed to bring this data together.

54. Other inhibiting factors included concern about disrupting a good working relationship with Police, and first mover disadvantage (the concern that revealing the extent of requests for information from law enforcement agencies might be negatively perceived by customers and put the company at a disadvantage relative to competitors that are not engaging in transparency reporting).

[8] Warrant powers to obtain content by compulsion are covered by Part 4 of the Intelligence and Security Act 2017.

55. However, we also received feedback from companies that they saw value in transparency reporting and in consolidating the way they receive and process requests for information. For companies that are considering making this investment in new business processes, we hope that the resources now available will make transparency reporting easier.

56. Along with this report, we are publishing guidance on the obligations of requestors and companies when making disclosures under the exceptions to principle 11 of the Privacy Act. You can find that guidance on our website (www.privacy.org.nz).

57. In 2018, we intend to launch a 'privacy tick' trust mark. Our aim is to create a way for consumers to know if they are using a service or product that will protect their privacy and personal information. The Privacy Tick is intended to be an endorsement by our Office of products and services which are designed with privacy in mind. Carrying out transparency reporting is the kind of privacy positive activity that could earn a company a 'privacy tick', for example for a standout report.