Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

Public Hearing – 23 May 2024

Questions on notice

Office of the Australian Information Commissioner Australian Privacy Commissioner

Question 1

Senator SHOEBRIDGE: Do you have any understanding of non-notification?

Ms Kind: I would say that, increasingly, the obligation on a modern privacy regulator is to not be in receipt of notifications of data breaches but rather to be actively trying to identify privacy interferences across the entire scope of that. In this case we are really only talking about security-related privacy issues, and there are many other principles, including privacy interferences at the stage of collection, use, disclosure et cetera that we would also need to be on the front food in identifying in order to sharpen up compliance across the ecosystem. And if we are waiting only for security incidents to alert us to instances of non-compliance, we are probably missing the entire iceberg under the water of privacy non-compliance. So a regulator like ours has to be on the front foot in that regard.

Senator SHOEBRIDGE: That is a big job though—

Ms Kind: it is.

Senator SHOEBRIDGE: To be out there proactively creating a pro-privacy culture. What sort of resources do you have to do that with? What is your budget for that part of your work?

Ms Kind: If you give me a minute, I'm sure I have that information. I might have to take the exact details of that on notice, Senator.

Senator SHOEBRIDGE: Yes. You can give an indication of headcount.

Ms Kind: Yes. The ASL is in the order of—and the reason I am less certain on this is that it is a movable feast in recent weeks—

Senator SHOEBRIDGE: You can tidy it up on notice—in the order of.

Ms Kind: If I may. Our headcount is in the order of 175 ASL, of which about—very generally; I'll come back to you with specifics—a third of those people are handling incoming complaints and investigations and a third are in policy and legal roles, interfacing with a range of different entities—

Senator SHOEBRIDGE: Writing submissions for bloody inquiries.

Ms Kind: Writing submissions for inquiries, briefing me, and then a third in corporate functions, such as communications, finance et cetera, and, of course, freedom of information, which is also part of our remit.

The response to the senator's question is as follows:

The Office of the Australian Information Commissioner (OAIC) continues to regulate information access and privacy rights in Australia. Our important regulatory work in the digital environment will be supplemented with an additional $5.6 million in funding in 2024–25 to ensure a robust regulatory approach to support the Australian Government's Digital ID initiative.

This budgetary enhancement partially offsets the impact of the 2024–25 Federal Budget on the OAIC with terminating funding measures at the end of the current financial year. This equates to approximately an $11 million net reduction of funding. These funds were allocated to the OAIC to allow it to undertake privacy regulatory functions which will continue, including in relation to social media and online platforms, and to investigate major data breaches such as the Optus, Medibank and Clinical Labs data breaches.

Going forward, the OAIC will work to inform and implement the Government's stated commitment to Australia's Privacy Act reform. Considering the support that this initiative will require, the OAIC will be working with the Government to ensure stable and sustainable funding to achieve our purpose of promoting and upholding privacy and information access rights.

The below table sets out the ASL*** and FTE**** by Branch as at 17 June 2024, including a description of the branch activities:

	Allocated staffing (ASL*) 2023-24***	**Allocation as % of total staffing**	**Forecast staffing (ASL***) 2023-24**	**Actual staffing (FTE****) as at 17-6-2024**	**% Split of FTE**** staffing by branch 17-6-24**
Regulation & Strategy Privacy and data regulatory advice and guidance, international engagement, assessments, Consumer Data Right, EDR Schemes	43.1	21%	33.4	34.0	17%
FOI Information Commissioner reviews, FOI complaints, extension of time applications, vexatious applicant declarations, FOI regulatory advice and guidance	32.3	16%	29.2	34.9	17%

	Allocated staffing (ASL***) 2023-24*	Allocation as % of total staffing	Forecast staffing (ASL***) 2023-24	Actual staffing (FTE****) as at 17-6-2024	% Split of FTE**** staffing by branch 17-6-24**
Dispute Resolution Privacy and FOI enquiries, privacy complaints, Notifiable Data Breaches scheme, privacy Commissioner initiated investigations	55.3	27%	49.9	54.2	27%
Major Investigations Commissioner Initiated Investigations (CIIs) which involve serious interferences with privacy and require complex investigations. Includes data breaches and other failures of cyber security resilience in APP entities. E.g. Medibank, Optus, ACL, Latitude Financial matters.	7.5	4%	10.6	11.6	6%
Corporate Strategic communications, people and culture, governance, risk, finance, information management, executive support, business analytics and reporting	29.6	14%	27.0	28.4	14%
Legal Services Legal services including all legal advice and litigation support, FOI applications on the OAIC.	18.2	9%	16.1	18.0	9%
Executive Information, Privacy and FOI Commissioners, Deputy Commissioner, COO, Assistant Commissioners, and support staff	14.1	7%	13.7	17.1	8%
Digital Identity Preparing for OAIC's role as privacy regulator for Australia's Digital ID system. As regulator OAIC will enforce privacy safeguards, undertake assessments, receive reports of data breaches, handle complaints, provide privacy advice, publish regulatory guidance.	5.0	2%	1.8	5.2	2%

** Refers to allocation of staffing in the management budget, which is Average Staffing Level (ASL).*

*** Rounded to nearest whole %*

**** ASL = average staffing level, is calculated as the average of the FTE's at each pay date during the financial year*

***** FTE = full time equivalent, is the number of staff adjusted for part time roles at any point in time*

Question 2

Senator SHOEBRIDGE: When you are investigating for potential privacy breaches by a big corporate—maybe there has been a big data theft—you might be investigating for privacy breaches by the corporate, and the state or federal police might be investigating the data theft itself. How does that work in practice—the cooperation, data sharing and information sharing?

Ms Kind: To my knowledge, we have not encountered challenges around data sharing between us and state or federal law enforcement.

Senator SHOEBRIDGE: Are there MOUs in place or some other arrangements that facilitate that?

Ms Kind: I don't believe there are MOUs. I can take that on notice and come back to you. But the tension lies elsewhere, I would suggest. In practice, when an entity, particularly a large entity, experiences a data breach, it is not that they know within 24 hours the scope, extent, impact and mitigation measures. That can take a year for them to fully interrogate and understand, depending on the complexity of their systems, whether it has been exfiltrated et cetera. So there is an ongoing investigative effort, usually internally, for the entity itself to understand what has happened. And then, running in parallel, there is our investigation, and then there are law enforcement investigations. So there is a challenge that we find in access to the information from the entities themselves.

The response to the senator's question is as follows:

The OAIC does not have any current formal arrangements (eg. Memoranda of Understanding) to facilitate cooperation with law enforcement agencies. The OAIC seeks to cooperate with law enforcement agencies, including the AFP, State and Territory law enforcement bodies, where relevant, when conducting its investigations. The OAIC recognises that there are limits to what can be shared with it by law enforcement agencies in the context of their conduct of a criminal investigation.

Section 33A of the *Privacy Act 1988*, provides an ability to share information or documents with enforcement bodies for the purpose of the Commissioner or the receiving body exercising their powers or performing their functions or duties.

Question 3

Senator SHOEBRIDGE: As I understand it, one of the problems of investigating is that, while you are getting your team together and perhaps issuing notices to produce or whatever the formal notice is, this data can literally be being churned.

Ms Kind: That is correct.

Senator SHOEBRIDGE: Destroyed and churned. Therefore, once a privacy breach is notified, clear statutory obligations to retain data and proactively provide them as part of the notification thing would seem to be kind of essential work we should be looking at.

Ms Kind: I would agree. I admit that I have not had conversations with my colleagues since starting in the role—as you know, only recently—as to whether they have thought through the potential disadvantages of such an approach. But, instinctively, having seen the challenges some investigators face, that would make sense.

Senator SHOEBRIDGE: Would you like to take that on notice and get back to us on what your experience is?

Ms Kind: Yes, thank you. I would appreciate that.

The response to the senator's question is as follows:

The OAIC notes there are different considerations regarding obligations to retain data logs, and whether there should be proactive disclosure of that data to the OAIC. In the OAIC's experience, the retention and availability of data logs is beneficial when conducting our investigations resulting from Notifiable Data Breaches (NDB). The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) provides entities with guidance on maintaining the integrity of evidence following a cyber security incident and the OAIC encourages entities to engage with the ACSC and take these steps to preserve evidence.

There is currently no specific legislative requirement to retain data logs and while there are various frameworks (for example, Essential 8) that have recommended timeframes for log retention, these also vary. From a broader investigative perspective, there is benefit to defining a minimum time frame for retaining event/data logs. When we commence preliminary inquiries with an entity following the notification of a data breach, the OAIC advises that there is a possibility for an investigation and requests the entity retain any records it holds or controls relating to the matter.

The OAIC notes that an obligation to proactively provide data or evidence to the OAIC as part of an NDB notification may discourage entities from complying with their notification obligations and could impact the timeliness of notifications. The OAIC uses its compulsive powers as required to obtain specific data relevant to its assessment of a suspected or actual eligible data breach or investigation and considers that a target approach to the provision of evidence to be preferable.

Question 4

Senator SHOEBRIDGE: And the parliament created some new offence provisions in some legislation, I think, at the end of 2022 or perhaps the be beginning of 2023, with significantly higher penalties. Has the office considered the use of those, or are they in the mix in any of these prosecutions or investigations?

Ms Kind: I will have to take that on notice. As I understand it, the 2022 amendments changed the scale of civil penalty that we can seek.

The response to the senator's question is as follows:

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*, which commenced on 13 December 2022, provided the Australian Information Commissioner with greater enforcement powers, including increased penalties for serious or repeated interferences with privacy under the *Privacy Act 1988*.

Of the six major investigations currently being undertaken by the OAIC, these new penalties will not be applicable in any current or potential proceedings against the entity by the Australian Information Commissioner in five of the matters as the alleged conduct occurred before the commencement of the updated penalty provisions. The increased penalties may be applicable in the OAIC's current major investigation of Latitude Financial.

Question 5

Senator SHOEBRIDGE: I know you've only got a head count of 175, so I feel low asking you to take a question on notice. Can you, though, take on notice just the basics of the current arrangements you have in place when you have dual prosecutions or investigations within the AFP and within the Privacy Commissioner and, if you can, address any similar arrangements you might have with states or territories. I don't require a forensic response to every jurisdiction but just what the nature of the arrangement is.

Ms Kind: At a high level, I know that our colleagues speak with the AFP frequently about the matters in which we have dual interest. I'll come back to you on the mechanics of that.

The response to the senator's question is as follows:

The OAIC's investigations are distinct from criminal investigation and prosecution by law enforcement agencies. The OAIC investigates serious breaches of the *Privacy Act 1988* and may take regulatory action including civil penalty proceedings, determinations and enforceable undertakings.

The OAIC does not have any current formal arrangements for dual investigations or prosecutions with law enforcement agencies. The OAIC has cooperated with law enforcement agencies, including the AFP, State and Territory law enforcement bodies, on a case-by-case basis when conducting its investigations.

The OAIC will seek to work in partnership with other regulators, recognising the practical and resource advantages in doing so. This may include agreeing to a written protocol or principles for collaboration, regular communication about privacy issues, sharing experience and coordinating the regulatory processes of the OAIC and other regulators.

The OAIC also has information sharing powers, including the ability to share information acquired in the exercise of its powers or performing its functions or duties under the *Privacy Act 1988* with enforcement bodies, alternative complaint bodies and privacy authorities of Australian State or Territory governments (s 33A).

Question 6

CHAIR: The Attorney-General's Department has work underway to reform Australia's electronic surveillance framework and to review computer offences. Do you have any recommendations or views on the law enforcement powers there over existing criminal offences that you would like to highlight? Considering, Commissioner, you're very new, I'm quite happy if you take that on notice and come back to us.

Ms Kind: Thank you, Senator. I'm aware we've been following that reform, and I don't think we've put forward any strong proposals about reforms that are needed, but I will take on notice whether or not there is something that my colleagues would like to bring forward as an answer to that question.

The response to the senator's question is as follows:

The OAIC has engaged with the Australian Government's consultation on reform of Australia's electronic surveillance legislation. The OAIC acknowledges the importance of intelligence agencies having access to electronic surveillance powers to protect national security and prevent serious crime, such as child sexual abuse and cybercrime.

The use of electronic surveillance powers involves intruding on the privacy of the person who is under surveillance and, in many cases, other people with whom that person interacts. The right to privacy is not absolute, and any interference with privacy must be prescribed by law, aimed at a legitimate objective, and reasonable, necessary and proportionate for that purpose.