GUIDING PRINCIPLES FOR SURVEILLANCE – CASE STUDIES

These hypothetical case studies have been prepared to provide examples of how the Guiding Principles for Surveillance can be applied and considered in projects or programs involving varying levels of surveillance.

Each case study assesses the acts or practices using the accompanying checklist. The facts of each case study may raise matters that go beyond privacy concerns, which are not considered.

CASE STUDY: USING A COMMUNICATION PLATFORM TO MONITOR EMPLOYEES

### **Background**

The Department of Digital Development’s employees are working from home.

All employees have migrated to using the Grapevine application to manage meetings and communications with colleagues.

Grapevine offers workspace chat and videoconferencing, file storage, application integration, and other useful tools that are essential to working from home.

### **User activity report**

Upon migrating to Grapevine, the software platform presented the Department of Digital Development’s unit managers with an option to receive weekly user activity reports for their employees.

The user activity reports provide unit managers with weekly, monthly and quarterly information, including:

* how many hours each employee’s Grapevine status is either active or away; and
* the number of Grapevine activities each employee has engaged in by activity type, including chat messages, private chat messages, calls and meetings.

Unit managers have not been provided with workplace guidance about the user activity reports and whether they should agree to receive them.

**Reporting surveillance concerns**

One Unit Manager recognises that receiving Grapevine user activity reports amounts to surveillance because the report will allow them to monitor and analyse their employee’s activity data to collect information pertaining to each individual team member’s movements and actions.

The Unit Manager reports their concerns to the Department’s Privacy Officer.

### **Analysis using the checklist**

The Privacy Officer is tasked with reviewing the privacy impacts of the user activity report, to assist the Department’s Executive team in deciding whether to use the report and if so, how it can be implemented in a privacy-enhancing way throughout the organisation.

In addition to conducting a privacy impact assessment, the Privacy Officer assesses the proposal to receive user activity reports against the Guiding Principles for Surveillance.

**Guiding Principles for Surveillance – Checklist**

|  |  |
| --- | --- |
| Program | Grapevine – User activity report |
| Organisation | Department of Digital Development |
| Date Completed | 20/03/2022 |

## **Legitimate aim**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **How does the surveillance connect or relate to the organisation’s functions or activities?**  *Any surveillance that collects personal information must only be done where it is necessary for a specific function or activity. Describe how it relates to the functions or activities of the organisation.* | No argument has been put forward to explain how the surveillance of employee activities through the user activity report is connected to the Department’s functions or activities.  The Privacy Unit considers the surveillance is not necessary to fulfil any specific function or activity of the organisation.  Even if the surveillance could be broadly characterised as relating to assurance activities, the type and level of surveillance is unnecessary to fulfil this function.  Of particular concern is the ongoing nature of the monitoring of all employees below a certain VPS level, the fact the monitoring may be covert if conducted without knowledge of the employees whom the reports are about, serious concerns around data quality, and the risks of inadvertent misuse or unfair use of the data. | **2.1** |
| **How will the organisation ensure personal information collected through surveillance is only used for the purpose for which it was collected?**  *Describe the policies, practices, or procedures that exist to ensure use is limited.* | No polices or procedures have been developed for the handling of personal information collected through user activity reports or other types of analytics reports available through the communications platform.  All personal information that may already have been collected through user activity reports should be destroyed as soon as practicable.  **Action item:** Permanently delete all information collected.  User activity reports should only be used by Unit Managers and employees if they are approved by the Executive team, after completion of a PIA.  The PIA will assist in ensuring that any proposed access, use and disclosure of personal information through user analytics reports is clearly understood and compliant with the IPPs. | **2.2** |

## **Necessity**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Why is the surveillance necessary to achieve the legitimate and lawful aim identified?** | No legitimate aim or outcome of receiving user activity reports has been identified.  The Privacy Unit does not consider the surveillance to be a necessary assurance activity to ensure compliance with internal policies or to assess workplace productivity.  There is no evidence to indicate the Department is experiencing issues with staff productivity or compliance with internal communication policies and processes. If there are concerns about these matters, the Privacy Unit considers there are already appropriate, less-intrusive assurance mechanisms available such as:   * internal policies and procedures, including the communications platform policy; * monitoring work outputs; and education, training, and awareness activities. | **3.1** |
| **Is it reasonable and practicable to collect the information directly from the individual, instead of using surveillance?**  *If yes, the information should not be collected through surveillance.* | The information in a user activity report is not collected directly from the individual. The Privacy Unit considers it would be reasonable and practicable to collect information of a similar nature directly from the individual, where a necessary reason to collect that information has been established. | **3.2** |

## **Proportionality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Has the proportionality of the surveillance required in the particular circumstances been considered?**  *Surveillance should be proportionate to the desired aim or outcome, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights. Surveillance should be limited to the least intrusive acts, practices, or methods necessary and only target relevant individuals. Alternative methods or strategies to achieve the desired aim or outcome should be considered.* | A legitimate aim has not been established against which to measure the proportionality of the surveillance.  Even if the surveillance could be broadly characterised as relating to assurance, the Privacy Unit considers that Unit Managers (and potentially other employees) receiving user activity reports of all employees within their team on an ongoing basis is not proportionate to achieve that goal.  No consideration has been given to who should be the subject of a user activity report and for what purpose.  Assuming the Department’s other assurance activities are not sufficient in a particular case, the Privacy Unit considers it likely that only *some* of the information contained in a user activity report may be necessary to collect on a *one-off or infrequent* basis for *specific employees*, not *all* information on an *ongoing* basis for *all employees*, as occurs with the user activity reports. | **4.1, 4.2, 4.3** |

## **Privacy Safeguards**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What steps are taken to provide individuals with notice of the surveillance?**  *Where personal information is collected through surveillance, reasonable steps must be taken to provide individuals with notice.* | No steps were taken to provide employees with notice that user activity reports about them would be accessed by their Unit Manager. The information required to be provided in a notice under IPP 1.3 was not provided.  Retrospective notice should be provided.  **Action item:** Provide notice to employees. | **5.2** |
| **Are policies and records in relation to the surveillance use published, including the purposes of surveillance and how collected personal information is used?** | No. The communications platform policy needs to be updated to incorporate information about user analytics reports.  **Action item:** Update communications platform policy. | **5.3, 5.4** |
| **Are individuals able to make a request for access to personal information collected through surveillance?**  *For example, through the Freedom of Information Act 1982 (Vic).* | The Department does have policies and procedures in place for employees to request their own personal information held by the Department. | **5.5** |
| **Does a process exist to either de-identify or destroy personal information collected through surveillance when it is no longer required?** | No documentation has been prepared. The Privacy Unit recommends all information collected to date is destroyed as soon as practicable.  **Action item:** Delete/destroy all information collected. | **5.6** |
| **If the personal information is being de-identified, has the risk of re-identification been assessed?**  *If the risk of re-identification cannot be reduced to very low, the information cannot be de-identified and should be destroyed when it is no longer required.* | No attempt is being made to de-identify the data. It is recommended that data is deleted/destroyed. | **5.7** |
| **Is anonymous information (rather than personal information) collected through surveillance wherever reasonably practicable?** | The user activity report inherently identifies the specific employee it is about. The report does not anonymise any information it generates. | **5.8** |
| **Is any information sharing limited to the purpose for the surveillance being undertaken?**  *Describe any information sharing that may or does occur and how it links to the purpose of surveillance being undertaken. A privacy impact assessment will assist to highlight areas of non-compliance.* | No guidance was provided to Unit Managers about the use and disclosure of user activity reports. If the Department does decide to use analytics reports in future, a PIA will need to be conducted prior to their use, to ensure information flows are clear. There will also need to be updates to internal policies and staff education to ensure that limits on use and disclosure are clearly understood.  **Action item:** Discuss issue at next Executive group meeting, to ensure Privacy Unit involvement in any future proposal to use analytics reports from the communication platform. | **5.9** |
| **Is personal information collected through surveillance stored in Victoria or a jurisdiction with equivalent privacy protections?**  *List other jurisdictions where personal information is held and explain why the protection is equivalent to Victoria, or why the transfer is otherwise permitted under IPP 9.* | The data servers of the communications platform are in a jurisdiction with equivalent privacy protections. The Privacy Unit’s analysis of transborder data flows is documented in the initial PIA of the platform. The Department’s data servers are located in Victoria. | **5.10** |
| **What steps are taken to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons?** | No steps were taken specific to the storage, use or disclosure of user activity reports. However, steps were specified in the PIA for the overall program. Employees are also subject to the Department’s Information Security Policy and Procedure, ICT Use Policy, and other relevant policies.  No further action is required at this time, if the information generated from user analytics reports is deleted in a timely manner. | **5.11** |
| **What resourcing has been allocated to ensure all safeguards are considered and effective?**  *Detail who is involved in the surveillance and their roles and responsibilities.* | The Privacy Unit considers resourcing is adequate. However, the short timeframe for the roll out of the communications platform meant that scrutiny of its features was not as thorough and diligent as it may otherwise have been.  The Privacy Unit considers it could have reviewed the PIA shortly after the Department began using the communications platform, to ensure any features of the platform that may have been missed or were unforeseen, were properly addressed. Communications could also have been sent to all staff advising them not to sign up to additional features of the platform without approval.  **Action items:**   * Add identified risks and risk mitigation strategies to risk register. * Add a step to our PIA process, to conduct an early review of a PIA for all short time frame proposals and projects. | **5.1** |

## **Non-discrimination**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance non-discriminatory with respect to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status?**  *Consider all stages of the information lifecycle, including any inferred information, and decisions made by the organisation that are based on the monitoring and analysis of surveillance data.* | The user analytics reports were only advertised to Unit Managers, meaning that only staff at a particular VPS level and below were subject to or could have been subject to surveillance.  There was no other consideration of attributes in the decision of who was to be subject to a user activity report. However, there is a real risk that interpretation of the data in a user analytics report by a Unit Manager could be discriminatory in some circumstances. For example, if the reports are analysed without consideration of other contextual information relevant to the employee and how and when they conduct their work. | **6.1** |

## **Legality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance lawful?**  *Ensure any applicable legal restrictions in enabling legislation and other state and Commonwealth legislation has been considered. This includes consideration of the Information Privacy Principles in the Privacy and Data Protection Act 2014 and the Charter of Human Rights and Responsibilities Act 2006.* | After updating the PIA, the Privacy Unit considers the use of the user activity report by unit managers and other Department employees to be in breach of the Information Privacy Principles in the *Privacy and Data Protection Act 2014* (Vic), and therefore not lawful. | **1.1, 1.3** |
| **Has a privacy impact assessment been undertaken?**  *See OVIC’s* [*Privacy Impact Assessment Guide and Template*](https://ovic.vic.gov.au/privacy/privacy-impact-assessment/)*.* | The Department’s Privacy Unit completed a privacy impact assessment (**PIA**) of the communication platform before the Department began using the platform. The PIA did not include an analysis of the platform’s analytics and reporting capability.  The PIA is being reviewed, to incorporate an analysis of this capability, and to update current and future privacy risks and mitigation strategies.  **Action Item:** Review and update privacy impact assessment. | **1.2** |
| **Is there a plan to periodically review the surveillance after implementation?**  *Describe where this plan or policy is documented and can be found, and who is responsible.* | The Privacy Unit had scheduled a review of the PIA, to occur 12 months after the Department began using the communication platform. This review is part of a wider review of the communication platform and policy by the Executive team.  The review plan is located on Content Manager and is owned by Corporate Services. | **1.4** |

## **Complaints and remedy**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What processes exist to ensure individuals are aware they can complain to the organisation and/or the Information Commissioner where they believe their privacy has been interfered with?** | Employees can complain to the Privacy Unit and staff are informed of how they can do this through information made available on the Intranet and regular reminders at all staff meetings.  A major issue with the user analytics reports is that employees were not made aware that Unit Managers were receiving the reports about them. In these circumstances, staff were unaware of the data collection and therefore unable to make a privacy complaint. | **7.1, 7.2** |

## **Recommendations / Action Items**

|  |  |
| --- | --- |
|  | **Recommendations / Action items** |
| **1** | Review and update privacy impact assessment if not already completed. |
| **2** | Immediately cease the use of user activity reports and any other analytics reports provided by the communications platform that have not already been pre-approved by the Executive. |
| **3** | Permanently delete all information collected. |
| **4** | Provide all employees affected with a detailed notice of what has occurred, why and what is being done. |
| **5** | Provide a general statement to unaffected employees to ensure it is clear to staff that non-approved analytics reports must not be used. |
| **6** | Add identified risks and risk mitigation strategies to risk register. |
| **7** | Review PIA policy and process to ensure an early review of a PIA is conducted for all short time frame proposals and projects in future. |
| **8** | Update communications platform policy to incorporate information about user analytics reports. |
| **9** | Speak to Executive group at next meeting, to discuss Privacy Unit involvement in any future proposal to use analytics reports from the communications platform. |

## **CASE STUDY: INSTALLING CCTV CAMERAS IN PUBLIC SPACES**

### **Background**

Quality City Council is fed up with a recent spate of vandalisms and thefts from motor vehicles around the Quality Library.

In response to the criminal activity, the Council is assessing strategies that may deter anti-social behaviour and criminal activity, and assist Police with identifying perpetrators.

One strategy proposes using closed circuit television (**CCTV**) surveillance cameras around the library to collect footage in areas where criminal activity is most likely to take place.

### **The proposal**

The cameras will monitor the entrances of the Quality Library, various pavement plaques in the gardens and the carpark, 24 hours a day.

The footage will be stored in a secure control room in the council’s offices and managed strictly in accordance with information security policies.

Access will only be given to council staff in the Security Unit and Police Officers who formally request access in relation to specific criminal incidents.

Use and disclosure of CCTV footage will be governed by Council’s existing CCTV policy, which limits uses to investigating and monitoring breaches of the law.

If no request is made to access footage collected within a 30-day period, the footage is destroyed.

### **Assessing the proposal**

The Council’s Privacy Officer has been tasked with reviewing the proposal. As well as conducting a privacy impact assessment the Privacy Officer is also assessing the proposal against the Guiding Principles for Surveillance.

**Guiding Principles for Surveillance – Checklist**

|  |  |
| --- | --- |
| Program | CCTV Cameras at entrance of Quality Library |
| Organisation | Quality City Council |
| Date Completed | 20/03/2022 |

## **Legitimate aim**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **How does the surveillance connect or relate to the organisation’s functions or activities?**  *Any surveillance that collects personal information must only be done where it is necessary for a specific function or activity. Describe how it relates to the functions or activities of the organisation.* | The installation of CCTV cameras is related to Council’s community safety functions, and obligations to maintain Council’s assets.  CCTV cameras are an effective strategy to deter anti-social behaviour and criminal activity. | **2.1** |
| **How will the organisation ensure personal information collected through surveillance is only used for the purpose for which it was collected?**  *Describe the policies, practices, or procedures that exist to ensure use is limited.* | Council is limiting access to footage to select members of our Council Security Unit. These members will strictly adhere to our CCTV footage use and disclosure policy, which limits any use to investigating and monitoring breaches of the law.  Our software retains access logs and requires staff to log in using unique logins. | **2.2** |

## **Necessity**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Why is the surveillance necessary to achieve the legitimate and lawful aim identified?** | Council is of the view that installation of the CCTV cameras is necessary to the achieve the aims outlined in point 2.1. Vandalism and theft are increasing exponentially, and research shows that CCTV cameras can have a significant impact on individuals’ willingness to commit crimes.  Council has investigated alternative options, including increasing patrols of local laws officers, and increasing lighting at night. While these options may be implemented, they are not considered as effective 24/7 deterrents. | **3.1** |
| **Is it reasonable and practicable to collect the information directly from the individual, instead of using surveillance?**  *If yes, the information should not be collected through surveillance.* | It is not possible to collect personal information from individuals directly. The CCTV cameras will monitor and record any individual that crosses into their line of sight. Personal information will be collected as part of footage being captured. | **3.2** |

## **Proportionality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Has the proportionality of the surveillance required in the particular circumstances been considered?**  *Surveillance should be proportionate to the desired aim or outcome, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights. Surveillance should be limited to the least intrusive acts, practices, or methods necessary and only target relevant individuals. Alternative methods or strategies to achieve the desired aim or outcome should be considered.* | The CCTV cameras will be focussed or directed towards specific areas of concern to reduce capturing individuals going about their daily lives.  Council has investigated alternative options, including increasing patrols of local laws officers, and increasing lighting at night. While these options may be implemented, they are not considered as effective 24/7 deterrents.  Council believes the installation of the CCTV cameras is the only available method to effectively monitor and reduce breaches of the law in the identified areas. | **4.1, 4.2, 4.3** |

## **Privacy Safeguards**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What steps are taken to provide individuals with notice of the surveillance?**  *Where personal information is collected through surveillance, reasonable steps must be taken to provide individuals with notice.* | Wherever CCTV cameras are installed, signage is also installed that details they belong to Council, a contact number for enquiries and requests, their purpose, and how any footage is used by Council.  **Action item:** Ensure appropriate signage is installed. | **5.2** |
| **Are policies and records in relation to the surveillance use published, including the purposes of surveillance and how collected personal information is used?** | Council maintains a CCTV policy detailing the locations of cameras, how and why they are used, and how footage is stored, used, disclosed, and destroyed.  **Action item:** Update CCTV policy to include information about these CCTV cameras. | **5.3, 5.4** |
| **Are individuals able to make a request for access to personal information collected through surveillance?**  *For example, through the Freedom of Information Act 1982 (Vic).* | Council complies with its obligations under the *Freedom of Information Act 1982* (Vic). | **5.5** |
| **Does a process exist to either de-identify or destroy personal information collected through surveillance when it is no longer required?** | Yes – Council policy requires footage to be deleted within 30 days unless required for investigating a breach of the law. The deletion process is automated and will be audited quarterly to ensure automatic deletion is occurring. | **5.6** |
| **If the personal information is being de-identified, has the risk of re-identification been assessed?**  *If the risk of re-identification cannot be reduced to very low, the information cannot be de-identified and should be destroyed when it is no longer required.* | Footage will not be de-identified. | **5.7** |
| **Is anonymous information (rather than personal information) collected through surveillance wherever reasonably practicable?** | By the very nature of capturing CCTV footage, personal information is recorded. It is not possible to record anonymous information. | **5.8** |
| **Is any information sharing limited to the purpose for the surveillance being undertaken?**  *Describe any information sharing that may or does occur and how it links to the purpose of surveillance being undertaken. A privacy impact assessment will assist to highlight areas of non-compliance.* | CCTV footage is only shared with Police for the purposes of investigating a breach of the law. Requests for access to CCTV footage are also processed lawfully under the FOI Act. | **5.9** |
| **Is personal information collected through surveillance stored in Victoria or a jurisdiction with equivalent privacy protections?**  *List other jurisdictions where personal information is held and explain why the protection is equivalent to Victoria, or why the transfer is otherwise permitted under IPP 9.* | Our data servers are located on Council premises. | **5.10** |
| **What steps are taken to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons?** | The footage will be stored in a secure control room in the council offices and managed strictly in accordance with information security policies.  Only council staff in the Security Unit can view the footage. Viewing the footage requires a unique login for each person and audit logs are retained.  Per Council policy, the footage will only be provided to Police when requested in relation to specific criminal incidents.  As an additional control, to copy or download the footage, the system requires two staff members to enter their unique login details. | **5.11** |
| **What resourcing has been allocated to ensure all safeguards are considered and effective?**  *Detail who is involved in the surveillance and their roles and responsibilities.* | These CCTV cameras will form part of Council’s existing CCTV program maintained and managed by our Security Unit. This unit is highly experienced in rolling out, using, maintaining, and reviewing Council’s use of CCTV cameras. | **5.1** |

## **Non-discrimination**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance non-discriminatory with respect to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status?**  *Consider all stages of the information lifecycle, including any inferred information, and decisions made by the organisation that are based on the monitoring and analysis of surveillance data.* | The CCTV cameras will record any individual who crosses into the cameras’ field of view. When capturing footage they do not discriminate based on any identified attributes. | **6.1** |

## **Legality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance lawful?**  *Ensure any applicable legal restrictions in enabling legislation and other state and Commonwealth legislation has been considered. This includes consideration of the Information Privacy Principles in the Privacy and Data Protection Act 2014 and the Charter of Human Rights and Responsibilities Act 2006.* | Commonwealth laws do not prohibit the installation of CCTV cameras in public spaces.  A privacy impact assessment is being concurrently developed to ensure compliance with the *Privacy and Data Protection Act 2014*. | **1.1, 1.3** |
| **Has a privacy impact assessment been undertaken?**  *See OVIC’s* [*Privacy Impact Assessment Guide and Template*](https://ovic.vic.gov.au/privacy/privacy-impact-assessment/)*.* | A privacy impact assessment is being concurrently developed to identify any risks and mitigation strategies.  **Action Item:** Complete privacy impact assessment and incorporate issues identified in this checklist. | **1.2** |
| **Is there a plan to periodically review the surveillance after implementation?**  *Describe where this plan or policy is documented and can be found, and who is responsible.* | Council policy requires all programs to be reviewed on a yearly basis. In addition, these CCTV cameras will form part of Council’s existing CCTV program maintained and managed by our Security Unit. | **1.4** |

## **Complaints and remedy**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What processes exist to ensure individuals are aware they can complain to the organisation and/or the Information Commissioner where they believe their privacy has been interfered with?** | Individuals can complain to the Privacy Unit and are informed of how they can do this through information made available on our website and privacy policy. | **7.1, 7.2** |

## **Recommendations / Action Items**

|  |  |
| --- | --- |
|  | **Recommendations / Action items** |
| **1** | Install clear and appropriate signage in obvious locations around CCTV cameras. |
| **2** | Update CCTV policy to include information about these CCTV cameras. |

## **CASE STUDY: RECORDING PRESENTATIONS AND CONFERENCES**

### **Background**

1. The Department of Incessant Symposiums conducts virtual presentations and conferences using the workplace communications application Grapevine
2. Employees often miss important presentations and conferences due to competing teleconferencing priorities.
3. During the last departmental pulse survey, employees expressed a strong desire for the Department to permit presentations and conferences to be recorded.

**Recording presentations and videoconferences**

1. The Department of Incessant Symposium’s Executive Leadership Team has proposed that, going forward, presentations and videoconferences are recorded via Grapevine to empower employees to catch-up on anything they miss.
2. However, some employees have raised concerns about their image or voice being captured if presenting or asking questions. The Public Engagement Unit has also noted that some conferences are open to members of the public, which may or may not complicate things.
3. The Executive Leadership Team has asked the Department’s Privacy Unit to review the proposal and highlight any surveillance risks, as well as make recommendations on next steps.

### **Assessing the proposal**

1. The Privacy Unit is conducting an initial assessment of the proposal using the Guiding Principles for Surveillance – Checklist, as well as completing a privacy impact assessment.

**Guiding Principles for Surveillance – Checklist**

|  |  |
| --- | --- |
| Program | Use of recording feature on Grapevine |
| Organisation | Department of Incessant Symposiums |
| Date Completed | 20/03/2022 |

## **Legitimate aim**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **How does the surveillance connect or relate to the organisation’s functions or activities?**  *Any surveillance that collects personal information must only be done where it is necessary for a specific function or activity. Describe how it relates to the functions or activities of the organisation.* | A core function of the Department is to provide for non-stop symposiums. Many of our presentations and conferences provide critical information to our staff or are related to staff development. Enabling the recording feature on Grapevine is an extension of our functions and activities.  However, this does not mean every presentation or conference should be recorded. Whether or not to record should be considered on a case-by-case basis. | **2.1** |
| **How will the organisation ensure personal information collected through surveillance is only used for the purpose for which it was collected?**  *Describe the policies, practices, or procedures that exist to ensure use is limited.* | Internal presentations and conferences will only be made available to view on the Department’s intranet.  There will be no option to download or further distribute the recording.  Any recording of a conference open to members of the public will be made available via the Department’s website.  Once published on the Department’s website, there is limited control over how these recordings might be used by members of the public, and any speakers will be informed of this. | **2.2** |

## **Necessity**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Why is the surveillance necessary to achieve the legitimate and lawful aim identified?** | Alternatives considered have included providing transcripts and presentation slides via the Department’s intranet and website.  The Department’s Communications Unit has advised this is unlikely to be effective. Past experiences have demonstrated transcripts and slide decks are infrequently accessed. They also noted staff have indicated via the ‘pulse survey’ that they would prefer being able to watch a video. | **3.1** |
| **Is it reasonable and practicable to collect the information directly from the individual, instead of using surveillance?**  *If yes, the information should not be collected through surveillance.* | All attendees are notified prior to any presentation or conference that will be recorded.  By default, all attendees will have their video and audio disabled. Additionally, any speakers or presenters will be asked if they consent to a recording being made. Where consent is not provided the recording will not take place. | **3.2** |

## **Proportionality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Has the proportionality of the surveillance required in the particular circumstances been considered?**  *Surveillance should be proportionate to the desired aim or outcome, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights. Surveillance should be limited to the least intrusive acts, practices, or methods necessary and only target relevant individuals. Alternative methods or strategies to achieve the desired aim or outcome should be considered.* | With the strategies noted above, the Privacy Unit considers enabling the recording feature to be proportionate.  There is no requirement for attendees to enable their video or audio, and speakers will be offered a choice to not record meetings. | **4.1, 4.2, 4.3** |

## **Privacy Safeguards**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What steps are taken to provide individuals with notice of the surveillance?**  *Where personal information is collected through surveillance, reasonable steps must be taken to provide individuals with notice.* | All participants will be provided with a notice advising that the host intends to record the presentation or conference. This will be included on any registration forms and meeting invitations.  Participants will also be advised of this at the beginning of any meeting or conference that is being recorded. | **5.2** |
| **Are policies and records in relation to the surveillance use published, including the purposes of surveillance and how collected personal information is used?** | While there is not a publicly available document setting out how and why recordings are made, a statement for the intranet and website will be developed and inserted on the relevant page hosting the recordings.  **Action item:** Develop statement outlining why and how recordings are made. | **5.3, 5.4** |
| **Are individuals able to make a request for access to personal information collected through surveillance?**  *For example, through the Freedom of Information Act 1982 (Vic).* | The Department complies with its obligations under the *Freedom of Information Act 1982* (Vic). In addition, all recordings will be available via the Department’s intranet and website. | **5.5** |
| **Does a process exist to either de-identify or destroy personal information collected through surveillance when it is no longer required?** | The Department does not intend to redact or edit recordings.  Presentation and conference will be retained until they are no longer considered useful. | **5.6** |
| **If the personal information is being de-identified, has the risk of re-identification been assessed?**  *If the risk of re-identification cannot be reduced to very low, the information cannot be de-identified and should be destroyed when it is no longer required.* | Recordings will not be de-identified. | **5.7** |
| **Is anonymous information (rather than personal information) collected through surveillance wherever reasonably practicable?** | Due to recording presentations and conferences, it is not possible to collect anonymous information only. The recordings will contain images and the voice of presenters. | **5.8** |
| **Is any information sharing limited to the purpose for the surveillance being undertaken?**  *Describe any information sharing that may or does occur and how it links to the purpose of surveillance being undertaken. A privacy impact assessment will assist to highlight areas of non-compliance.* | As noted, recordings will be made available to view via the Department’s intranet and website. While downloading the recordings will be disabled it is impossible to stop the recording being used for other unforeseen downstream purposes. | **5.9** |
| **Is personal information collected through surveillance stored in Victoria or a jurisdiction with equivalent privacy protections?**  *List other jurisdictions where personal information is held and explain why the protection is equivalent to Victoria, or why the transfer is otherwise permitted under IPP 9.* | Our data servers are located on premise. | **5.10** |
| **What steps are taken to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons?** | As noted, recordings will be made available to view via the Department’s intranet and website. While downloading the recordings will be disabled it is impossible to stop the recording being used for other unforeseen purposes. | **5.11** |
| **What resourcing has been allocated to ensure all safeguards are considered and effective?**  *Detail who is involved in the surveillance and their roles and responsibilities.* | Presentation and conference hosts will be responsible for enforcing the Department’s Grapevine policy, i.e., ensuring appropriate consents and notices are provided. Template consents and notices will be made available in the Grapevine policy.  **Action item:** Develop template consents and notices. | **5.1** |

## **Non-discrimination**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance non-discriminatory with respect to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status?**  *Consider all stages of the information lifecycle, including any inferred information, and decisions made by the organisation that are based on the monitoring and analysis of surveillance data.* | To the Department’s knowledge, Grapevine recording does not discriminate when recording. | **6.1** |

## **Legality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance lawful?**  *Ensure any applicable legal restrictions in enabling legislation and other state and Commonwealth legislation has been considered. This includes consideration of the Information Privacy Principles in the Privacy and Data Protection Act 2014 and the Charter of Human Rights and Responsibilities Act 2006.* | Commonwealth laws do not prohibit the Department from enabling the recording feature of Grapevine.  A privacy impact assessment is being undertaken to determine compliance with the IPPs and identify any risks and mitigation strategies. | **1.1, 1.3** |
| **Has a privacy impact assessment been undertaken?**  *See OVIC’s* [*Privacy Impact Assessment Guide and Template*](https://ovic.vic.gov.au/privacy/privacy-impact-assessment/)*.* | A privacy impact assessment is being concurrently developed to identify any risks and mitigation strategies.  **Action Item:** Complete privacy impact assessment and incorporate issues identified in this checklist. | **1.2** |
| **Is there a plan to periodically review the surveillance after implementation?**  *Describe where this plan or policy is documented and can be found, and who is responsible.* | If the recording feature is enabled, the ‘Use of Grapevine’ policy will be updated to reflect this new use. Departmental policy dictates all policies are reviewed on a 12-month schedule.  **Action item:** Update Grapevine policy. | **1.4** |

## **Complaints and remedy**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What processes exist to ensure individuals are aware they can complain to the organisation and/or the Information Commissioner where they believe their privacy has been interfered with?** | Employees can complain to the Privacy Unit and are informed of how they can do this through information made available on our intranet and privacy policy. | **7.1, 7.2** |

## **Recommendations / Action Items**

|  |  |
| --- | --- |
|  | **Recommendations / Action items** |
| **1** | Complete PIA on the use of the recording feature. |
| **2** | Update Grapevine policy to note the conditions of use of the recording feature. |
| **3** | Develop template for speaker consent and notice that recording feature will be used. |
| **4** | Develop statement outlining why and how recordings are made for website and intranet. |

CASE STUDY: MONITORING PRODUCTIVITY AND COMPLIANCE IN THE WORKPLACE

### **Background**

The Department of State Security’s employees are working from home.

O’Brien, the Department of State Security’s Chief of Staff, worries that employees are loafing about, baking sourdough, and brazenly napping while their inboxes are reaching critical mass. O’Brien also worries that employees could be emailing sensitive documents to their personal email accounts, in violation of the Department’s information security policy.

### **A clandestine solution**

In response to his concerns, O’Brien procures surveillance software from Bossware Analytics Propriety Unlimited.

Without informing the Department of State Security’s employees, O’Brien arranges for the software to be installed on all work-issued computers during the next-scheduled software update.

The software allows O’Brien to monitor keystrokes and mouse movements of the Department’s computers, scrape emails, and take screenshots of employee screens.

### **All staff meeting**

Several months later, O’Brien has collected sufficient information to conclude that employees are in fact maintaining productivity while working from home. However, O’Brien has also collected information indicating that two employees, Carrie and Steve, have violated information security protocols by sending sensitive documents to their personal email accounts.

After referring Carrie and Steve to disciplinary action, O’Brien convenes an online all staff meeting to congratulate the Department of State Security’s employees for their enduring productivity. O’Brien informs the employees that he has confirmed their productivity levels by having people analytics software installed during a software update.

The Department of State Security’s employees are furious with O’Brien and they complain to the Department’s Privacy Officer.

### **Analysis using the checklist**

The Department’s Privacy Unit, who was not consulted, is now involved and retrospectively considering the privacy impacts of O’Brien’s decision to install the surveillance software in the context of the Guiding Principles for Surveillance.

**Guiding Principles for Surveillance – Checklist**

|  |  |
| --- | --- |
| Program | Bossware Analytics Propriety Unlimited – Monitoring Software |
| Organisation | Department of State Security |
| Date Completed | 20/03/2022 |

## **Legitimate aim**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **How does the surveillance connect or relate to the organisation’s functions or activities?**  *Any surveillance that collects personal information must only be done where it is necessary for a specific function or activity. Describe how it relates to the functions or activities of the organisation.* | Conducting covert surveillance based on one person’s belief that staff would not work productively from home is not connected to the functions or activities of the Department.  The surveillance might be broadly characterised as relating to the assurance activities of the Department, to ensure staff are complying with the Department’s information security policies.  However, the type and level of surveillance is clearly unnecessary to fulfil the assurance function – namely the ongoing, covert, and indiscriminate monitoring of the keystrokes and mouse movements of the Department’s computers, scraping emails, and taking screenshots of employee screens. | **2.1** |
| **How will the organisation ensure personal information collected through surveillance is only used for the purpose for which it was collected?**  *Describe the policies, practices, or procedures that exist to ensure use is limited.* | No polices or procedures have been developed for the handling of personal information collected by the Chief of Staff.  All personal information that has been collected should be destroyed immediately. It is likely that confidential and sensitive information has been collected, such as personal logins and passwords.  The Privacy Unit considers this to be a significant risk to both the staff and the organisation.  **Action item:** Permanently delete all information collected.  A PIA must be conducted for any future proposal to use people analytics software, to ensure that the proposed access, use and disclosure of personal information is clearly understood and compliant with the IPPs. | **2.2** |

## **Necessity**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Why is the surveillance necessary to achieve the legitimate and lawful aim identified?** | The Privacy Unit does not consider that the surveillance is a necessary assurance activity to ensure compliance with the Department’s information security policy or to assess workplace productivity.  There is no evidence to indicate the Department was experiencing issues with staff productivity or compliance with the information security policy before the surveillance was implemented. Further, no consideration was given to how covert surveillance would or could assist in maintaining workplace productivity. | **3.1** |
| **Is it reasonable and practicable to collect the information directly from the individual, instead of using surveillance?**  *If yes, the information should not be collected through surveillance.* | Given the type of surveillance undertaken it would not have been possible to collect personal information directly from individuals. However, it is noted that alternative methods may have been available allowing productivity information to be collected directly from individuals. | **3.2** |

## **Proportionality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Has the proportionality of the surveillance required in the particular circumstances been considered?**  *Surveillance should be proportionate to the desired aim or outcome, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights. Surveillance should be limited to the least intrusive acts, practices, or methods necessary and only target relevant individuals. Alternative methods or strategies to achieve the desired aim or outcome should be considered.* | The installation of the monitoring software was not proportionate. The Privacy Unit is of the view that alternative strategies or less intrusive monitoring could have been considered.  The Privacy Unit considers there were already appropriate mechanisms available such as:   * monitoring work outputs; and * education, training, and awareness activities on information security. | **4.1, 4.2** |

## **Privacy Safeguards**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What steps are taken to provide individuals with notice of the surveillance?**  *Where personal information is collected through surveillance, reasonable steps must be taken to provide individuals with notice.* | No steps were taken to provide employees with notice that the software would be installed, and of the other information required to be provided in the notice under IPP 1.3. This is in breach of IPP 1.3. | **5.2** |
| **Are policies and records in relation to the surveillance use published, including the purposes of surveillance and how collected personal information is used?** | No policies or procedures were developed. | **5.3, 5.4** |
| **Are individuals able to make a request for access to personal information collected through surveillance?**  *For example, through the Freedom of Information Act 1982 (Vic).* | The Department does have policies and procedures in place for requesting access to personal information held by the Department. However, it is unlikely many of our employees are aware of these processes.  **Action item:** Improve staff awareness of their ability to request access to their own personal information held by the Department. | **5.5** |
| **Does a process exist to either de-identify or destroy personal information collected through surveillance when it is no longer required?** | No documentation has been prepared. The Privacy Unit recommends all information collected to date is immediately destroyed.  **Action item:** Delete/destroy all information collected. | **5.6** |
| **If the personal information is being de-identified, has the risk of re-identification been assessed?**  *If the risk of re-identification cannot be reduced to very low, the information cannot be de-identified and should be destroyed when it is no longer required.* | No attempt is being made to de-identify the data. It is recommended that data is deleted/destroyed. | **5.7** |
| **Is anonymous information (rather than personal information) collected through surveillance wherever reasonably practicable?** | Anonymous information cannot and was not collected via the software. | **5.8** |
| **Is any information sharing limited to the purpose for the surveillance being undertaken?**  *Describe any information sharing that may or does occur and how it links to the purpose of surveillance being undertaken. A privacy impact assessment will assist to highlight areas of non-compliance.* | N/A | **5.9** |
| **Is personal information collected through surveillance stored in Victoria or a jurisdiction with equivalent privacy protections?**  *List other jurisdictions where personal information is held and explain why the protection is equivalent to Victoria, or why the transfer is otherwise permitted under IPP 9.* | While our data servers are located in Victoria, it appears the Chief of Staff was under a mistaken impression as to where the data would be stored. On closer inspection of Bossware’s policy it is apparent that all data has been processed and is being stored by Bossware in undisclosed foreign countries.  We are unable to determine if the data is stored in a jurisdiction with equivalent privacy protections.  Fortunately, it does appear we are able to delete the data via the Chief of Staff's account.  **Action item:** Permanently delete all information collected. | **5.10** |
| **What steps are taken to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons?** | The Privacy Unit has identified that limited information security practices were implemented. There is no clear project owner, and access to the information collected is available to view, download, and delete through a shared password.  **Action item:** Conduct an information security risk assessment. | **5.11** |
| **What resourcing has been allocated to ensure all safeguards are considered and effective?**  *Detail who is involved in the surveillance and their roles and responsibilities.* | The Privacy Unit does not believe adequate resourcing was allocated at the start of this project. Privacy, security, risk and assurance policies and assessments have not been followed to date.  Aside from the Chief of Staff, a project owner, with day-to-day oversight, has not been identified. | **5.1** |

## **Non-discrimination**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance non-discriminatory with respect to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status?**  *Consider all stages of the information lifecycle, including any inferred information, and decisions made by the organisation that are based on the monitoring and analysis of surveillance data.* | The software collected personal information from all staff with no consideration of attributes. | **6.1** |

## **Legality**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **Is the surveillance lawful?**  *Ensure any applicable legal restrictions in enabling legislation and other state and Commonwealth legislation has been considered. This includes consideration of the Information Privacy Principles in the Privacy and Data Protection Act 2014 and the Charter of Human Rights and Responsibilities Act 2006.* | The covert installation of the software is a breach of the Information Privacy Principles in the *Privacy and Data Protection Act 2014* (Vic) and therefore unlawful.  In addition, the Legal Unit has been requested to assess whether any other Commonwealth or State laws have been breached. | **1.1, 1.3** |
| **Has a privacy impact assessment been undertaken?**  *See OVIC’s* [*Privacy Impact Assessment Guide and Template*](https://ovic.vic.gov.au/privacy/privacy-impact-assessment/)*.* | The Department’s Privacy Unit was not consulted, and a Privacy Impact Assessment (**PIA**) has not been undertaken.  A PIA will be developed to identify existing and future risks, and mitigation strategies.  **Action Item:** Conduct a PIA. | **1.2** |
| **Is there a plan to periodically review the surveillance after implementation?**  *Describe where this plan or policy is documented and can be found, and who is responsible.* | The Chief of Staff did not implement or develop a program to review the installation and monitoring of staff. If a decision is made to continue using this software a review plan must be developed. | **1.4** |

## **Complaints and remedy**

|  |  |  |
| --- | --- | --- |
| **Question** | **Response** | ***Guiding Principle*** |
| **What processes exist to ensure individuals are aware they can complain to the organisation and/or the Information Commissioner where they believe their privacy has been interfered with?** | Employees can complain to the Privacy Unit and are informed of how they can do this through information made available on our intranet and privacy policy.  In this instance employees will be advised email of what has occurred, what actions the Department is undertaking, as well as information on their complaint rights. | **7.1, 7.2** |

## **Recommendations / Action Items**

|  |  |
| --- | --- |
|  | **Recommendations / Action items** |
| **1** | Conduct a privacy impact assessment of the Department’s use of the software. |
| **2** | Immediately cease the use of the software. |
| **3** | Permanently delete all information collected. |
| **4** | Provide all employees with a detailed notice of what has occurred, why and what is being done. |
| **5** | Update information on Intranet about the ability for staff to request access to their own personal information held by the Department and include a segment on this at the next all staff meeting. |
| **6** | Conduct an information security risk assessment following the decision to stop using the software. |