OneTrust

Privacy Management Software

Assessment Summary Report

GrayKey

Created On: Mon Sep 17 19:38:49 GMT 2018
Created By: Jimi Robinson

OneTrust
Privacy Management Software

Assessment Summary Report

GrayKey

GrayKey is used to allow access to iPhones that are locked for forensic purposes.

Creator / Date Created
Jimi Robinson / Mon Sep 17 19:38:49 GMT 2018

Status / Deadline
Under Review / Fri Sep 21 07:00:00 GMT 2018

Respondent / Submitted Date
Jimi Robinson / Mon Sep 17 19:48:32 GMT 2018

Organization
Privacy

Approver / Approval Date
Ginger Armbruster /

Template / Version
Privacy and Surveillance Assessment / 12

Assessment

1 Description

1.1 Title
Please be as descriptive as possible. Generic answers such as "technology," "intern," etc. will not be accepted

Response

GrayKey

1.2 Description
Please attach applicable documentation for contracts, surveys, Adobe Sign, etc.

Response

This solution will be used to access locked iPhones for forensic use by the Seattle Police Department.

1.3 Project Manager/ Primary Contact

Response

CSD: Jimi Robinson SME Captain Mike Edwards Seattle Police Department High Risk Victims Section Commander WA ICAC Task Force Commander WA HT Task Force Commander 610 Fifth Avenue Seattle, WA 98104-4986 (206) 684-4351 (desk) (206) 786-2762 (cell)

1.4 Customer Department

Response

SPD

Justification

1.5 Type
Please note, IT Portfolio Projects are reviewed through a separate assessment titled "IT Portfolio Project Review".

Response

Purchase Intake Request - PIR

Justification

1.6 IT Project Portfolio ID number

Skipped

1.7 Concept Stage Notes

Skipped

1.8 Initiation Stage Notes

Skipped

1.9 Planning Stage Notes

Skipped

1.10 Execution Stage Notes

Skipped

1.11 Closeout Notes

Skipped

1.12 **PIR Number**

Response

2-1290-18

2 Privacy Assessment

2.1 **Will members of the public interact with the system (i.e. will the system collect or store information about the public)?**
For example, will the public input information, or will City staff input information about/for the public? This may include contractors or businesses.

Response

No

Justification

2.2 **Is this standard hardware or software?**
Click here to see which tools are standard. Contact ITD_SP_EAO@seattle.gov if you have any questions. Please note that a technology will only be considered standard if it appears on this list.

Response

No

Justification

2.3 **Will this only collect City of Seattle employee and/or City infrastructure data?**

Response

No

Justification

2.4 **What personal information is being used or collected? Please select one or more of the applicable data options below**
For more information on what "personally identifiable information" is, please visit the Privacy Toolkit.

Response

Data stored on mobile phone.

Justification
This solution has the ability to access any data that is held on a cell phone. After the device is unlocked, the full contents of the filesystem are downloaded to the GrayKey device. From there, they can be accessed through a web-based interface on a connected computer, and downloaded for analysis.

2.5 **Are you only collecting the data or information that you need? Describe how the information used or collected is necessary to meet a service or business requirement.**
Describe how the information used or collected is necessary to meet a service or business requirement.

Response

After the device is unlocked, the full contents of the filesystem are downloaded to the GrayKey device. This purchase is necessary for the forensic investigation of ICAC (Internet Crimes Against Children) cases.

2.6 **Are you telling users/ the public what information you are collecting and how it will be used? Do you provide notice of public disclosure?**
Include the actual language and where in the data collection process it occurs. If no notice is provided, explain why not (e.g., for certain law enforcement project/technologies, notice may not be appropriate). You may access Privacy-approved notice language here.

Response

There are three use cases for acquiring iPhones in the course of running investigations for the Internet Crimes Against Children Task Force (ICAC). The first two, Voluntary Surrender and Request for Search require a signed consent form from the iPhone owner. The third, Service of a Search Warrant for recovery of information, is the only use case that would use this technology and this involves service of a search warrant and an itemized receipt of all items recovered in the search that goes to both the individual and the court. All use cases involve consent or notice.

2.7 **Can the users/ the public opt out of providing any of the data requested?**
For example, are there required or non-required fields? If this is not an option, please explain why.

Response

No, this technology is used in forensic investigations and so opting-out is not an option.

2.8 **Will a third party be engaged?**
For example, a vendor, contractor, developer, academic researchers, etc. If so, what privacy and security language is in the agreement? You may access Privacy-approved examples here.

Response

The vendor may be engaged for training and issue resolution.

2.9 **Is the data going to be shared, either between City departments or outside entities? If so, what is the intended purpose or requirement for data sharing?**

Response

This solution is used for Forensic purposes only. Data sharing may be required in the process of an investigation between members of the ICAC Task Force and external law enforcement bodies.

2.10 **What is the Security, Risk and Compliance (SRC) Review status for this project?**
Please ensure SRC is engaged in the review process. If you are unsure whether this needs an SRC review, please contact ITD_SRC_Intake@seattle.gov.

Response

Data is not accessed from computers connected to the SPD/City network.

2.11 **What is the City Records Management Program (CRMP) Review status for this project?**
For more information, please visit the City Records Management InWeb Site. To complete the review, please contact Jennifer.Winkler@seattle.gov

Response

The retention policy of this data follows regular SPD investigation retention requirements.

3 Surveillance Assessment

3.1 **Is the purpose to observe or analyze the movements, behavior, or actions of member of the public?**
This may include images, audio, or video of identifiable individuals.

Response

No

Justification
This solution is used for forensic purposes only.

3.2 **Is this a technology that is used to collect data where an individual knowingly and voluntarily provides the data?**
For example, individuals sign a consent form.

Skipped

Justification
This solution is used for Forensic purposes only. Please reach out to Capt. Edwards for more detail.

3.3 **Is this a technology that is used to collect data where individuals were presented with a clear and conspicuous opt-out notice?**

Skipped

Justification
This solution is used for Forensic purposes only. Please reach out to Capt. Edwards for more detail.

3.4 **Is this a technology used for everyday office use?**

Skipped

Justification

3.5 **Is the technology SPD's body-worn cameras?**

Skipped

Justification

3.6 **Is the technology a camera installed in or on a police vehicle?**

Skipped

Justification

3.7 **Is the technology a camera(s) installed pursuant to state law authorization in or on any vehicle or along a public right-of way solely to record traffic violations?**

Skipped

Justification

3.8 **Is the technology a camera installed on City property solely for security purposes?**

Skipped

Justification

3.9 **Is the technology a camera(s) installed solely to protect the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs?**

Skipped

Justification

3.10 **Is the technology solely monitoring City employees in the performance of their City functions?**

Skipped

Justification

3.11 **Does the technology disparately impact disadvantaged groups?**

Skipped

Justification
This solution is used for Forensic purposes only. Please reach out to Capt. Edwards for more detail.

3.12 **Is there a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service?**

Skipped

Justification
This solution is used for Police case forensic purposes only. Please reach out to Capt. Edwards for more detail.

3.13 **Does the technology collect data that is personally identifiable even if obscured, de-identified, or anonymized after collection?**

Skipped

Justification
This solution is used for Police case forensic purposes only. Please reach out to Capt. Edwards for more detail.

3.14 **Might the technology raise reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice?**

Skipped

Justification
This solution is used for Police case forensic purposes only. Please reach out to Capt. Edwards for more detail.

4 STOP AND SUBMIT

4.1 **You have completed the Privacy and Surveillance Assessment.**
You will not be able to press "submit" until all the required fields have been completed. Look at the left side navigation for any red asterisks (*) to navigate to the section with a required field that has not yet been answered.

If the problem persists, please refresh the page - all your content will still be saved.

5 Privacy Review Notes

5.1 **Date of Initial Privacy Review**

9/17/2018 7:00:00 AM

5.2 **Privacy Approval Status**

Not Answered

Justification

5.3 **Surveillance Determination**

Response

This project technology does not meet the definition of surveillance technology. This is based on the current information available. The determination is subject to change based on new information or City Council action.

Justification

5.4 **Privacy Risk**

Response

High

Justification

5.5 **Privacy Impact Assessment**

Response

Required, in progress

Justification

5.6 **Approved for PIR?**

Not Answered

Justification

5.7 **Approval to move from concept to initiation**

NotSure

5.8 **Approval to move from initiation to planning**

NotSure

5.9 **Approval to move from planning to execution**

NotSure

5.10 **Approval to move from execution to closeout**

NotSure

Notes

Ginger Armbruster *Fri Sep 21 16:22:15 GMT 2018*
Everyone

9/21/2018 Left VM with Capt Edwards to discuss how this fits into the surveillance ordinance. If phones are acquired either under warrant or with suspects knowledge then this is not surveillance by ordinance definition. Need to clarify this in order to proceed.

Ginger Armbruster *Mon Oct 08 19:07:39 GMT 2018*
Everyone

10/8/2018: Meeting with Gary Smith in Law 10/9 to get legal determination about surveillance.

Ginger Armbruster *Mon Oct 15 19:40:41 GMT 2018*
Everyone

Date: 9/26

Email to Capt. Edwards and Jimi,

Thank you for sending me the policy and case law information about police searches. As we discussed, GrayKey does not meet the current definition of a surveillance technology. After further consideration, however, there is still a high privacy risk associated with this technology that will be of public and Council interest. Therefore, we are requesting that SPD complete a PIA (Privacy Impact Assessment) before approving for purchase.

I believe that you have much of the documentation to complete the PIA and I am copying SPD Privacy as they are tasked with completing these more highly detailed reviews and is familiar with the requirements. We will do whatever we can to expedite the completion of the review for this request. I am attaching the PIA template to get this started.

Ginger Armbruster
Chief Privacy Officer

Nathan Merrells *Thu Oct 04 18:16:13 GMT 2018*
Everyone

9/27/2018: We have requested a PIA from Mary Perry to document the policies and use of the technology. Once we have received and reviewed this we will be able to approve.

GrayKey is used with either individual consent or notice, the last in cases of search warrant. While there are other privacy and legal considerations for the use of this technology, the policies around obtaining the mobile devices under consent or via warrant place this technology outside of Surveillance Ordinance.