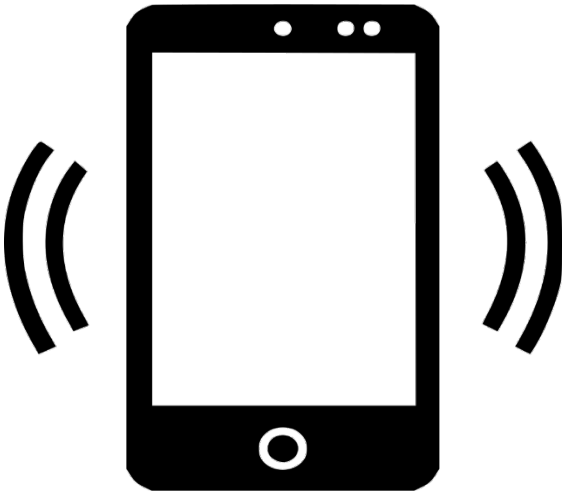
Callyo

Seattle Police Department (SPD)

¿En qué consiste esta tecnología?

Callyo es una tecnología de grabación y enmascaramiento de identificación de teléfonos celulares que se utiliza solo con una orden judicial. Callyo se instala en un teléfono celular y permite ocultar la identidad de un oficial mediante el enmascaramiento del número de teléfono, grabar conversaciones telefónicas y localizar personas identificables por GPS (global



¿Por qué utilizamos esta tecnología?

Callyo permite al Seattle Police Department (SPD, Departamento de Policía de Seattle) procurar resolver las investigaciones penales con rapidez mediante el enmascaramiento del número de teléfono de un participante voluntario en una investigación encubierta, la grabación de conversaciones y el registro de la ubicación de los sospechosos. Los dispositivos de grabación de audio se utilizan solo después de que se hayan cumplido los estándares legales de consentimiento o una orden judicial emitida por un tribunal, como lo requiere la Washington Privacy Act (Ley de Privacidad de Washington), cap. 9.73 del Revised Code of Washington (RCW, Código Revisado de Washington). La grabación de audio de Callyo y el enmascaramiento del número de teléfono contribuyen a la reducción del delito, ya que ayudan a reunir pruebas relacionadas con actividades delictivas graves o violentas como parte de la investigación de la actividad delictiva. Sin esta tecnología, el SPD no podría reunir pruebas importantes en algunas investigaciones penales.

Se encuentra abierto el período para recibir comentarios del público sobre esta tecnología. Puede enviar sus comentarios a **Seattle.gov/Surveillance**.

Todos los comentarios se incluirán en el "Informe del efecto de la vigilancia" sobre esta tecnología y se presentarán ante el Consejo.

Si le gustaría compartir comentarios fuera del período abierto para recibir comentarios del público, preséntelos directamente al Consejo de la ciudad.

Obtención

Cuando se utiliza Callyo para grabar, esta tecnología obtiene conversaciones y sonidos de personas relacionadas con una investigación penal. Los datos obtenidos por Callyo se proporcionan al oficial o detective solicitante para que se incluyan en el archivo de investigación y se almacenen de acuerdo con las directrices de evidencia.

Uso

La High Risk Victims Unit (Unidad de Víctimas de Alto Riesgo) utiliza Callyo para enmascarar números de teléfono, pero no utiliza las funciones de grabación de Callyo. Para todas las demás implementaciones de Callyo, después de haber establecido la causa probable, los oficiales presentan una solicitud verbal a la TESU para la implementación de Callyo. La TESU documenta el equipo solicitado, la autoridad legal y el número de caso. Luego, la TESU brinda el equipo al oficial o detective solicitante para que lo utilice dentro del ámbito de aplicación de la orden judicial.

Protecciones

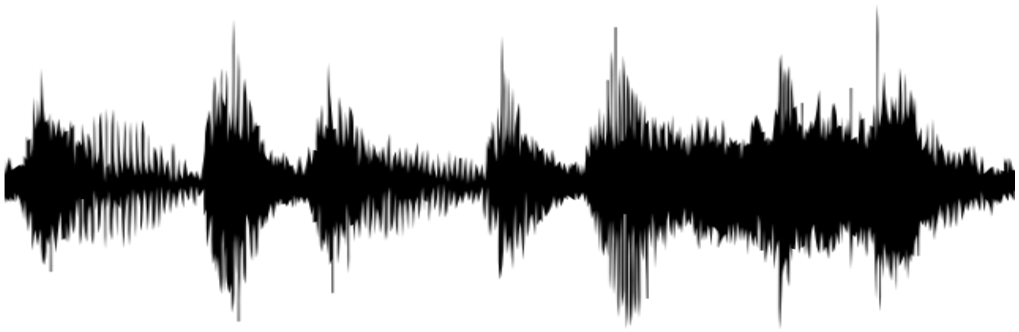
La implementación de los dispositivos de grabación de audio está restringida a las condiciones previstas por el consentimiento o la orden judicial, que proporcionan la autoridad legal y el ámbito de aplicación de los datos obtenidos. Los dispositivos de grabación de audio se utilizan solo después de que se hayan cumplido los estándares legales de consentimiento o una orden judicial emitida por un tribunal, como lo requiere la Washington Privacy Act, cap. 9.73 del RCW. Además, todas las implementaciones de los dispositivos de grabación de audio están documentadas por la TESU y están sujetas a auditoría por parte de la Office of Inspector General (Oficina del Inspector General) y el supervisor federal en cualquier momento.

Sistemas de grabación de audio (“micrófonos”)

Seattle Police Department (SPD)

¿En qué consiste esta tecnología?

Los dispositivos de grabación de audio se conocen normalmente como “micrófonos” y pueden ocultarse en una persona o esconderse en o sobre objetos en un entorno particular. Los dispositivos de grabación de audio deben ser activados por una persona y solo graban partes de una conversación que se lleva a cabo mientras el dispositivo está encendido. Los dispositivos de grabación de audio se utilizan solo después de que se hayan cumplido los estándares legales de consentimiento o una orden judicial emitida por un tribunal, como lo requiere la Washington Privacy Act (Ley de Privacidad de Washington), cap. 9.73 del Revised Code of Washington (RCW, Código Revisado de Washington).



Se encuentra abierto el período para recibir comentarios del público sobre esta tecnología. Puede enviar sus comentarios a **Seattle.gov/Surveillance**.

Todos los comentarios se incluirán en el “Informe del efecto de la vigilancia” sobre esta tecnología y se presentarán ante el Consejo.

Si le gustaría compartir comentarios fuera del período abierto para recibir comentarios del público, preséntelos directamente al Consejo de la ciudad.

¿Por qué utilizamos esta tecnología?

Los sistemas de grabación de audio permiten al Seattle Police Department (SPD, Departamento de Policía de Seattle) procurar resolver las investigaciones penales con rapidez, grabando las conversaciones de los sospechosos una vez que se ha tomado una decisión correspondiente de que existe suficiente causa probable y se ha emitido una orden judicial. Por ley, se requiere causa probable para obtener una orden de registro. Los sistemas de grabación de audio contribuyen a la reducción del delito, ya que ayudan a reunir pruebas relacionadas con actividades delictivas graves o violentas como parte de la investigación de la actividad delictiva.

Obtención

Los dispositivos de grabación de audio obtienen conversaciones y sonidos de personas relacionadas con una investigación penal. Los datos obtenidos de los dispositivos de grabación de audio se proporcionan al oficial o detective solicitante para que se incluyan en el archivo de investigación y se almacenen de acuerdo con las directrices de evidencia.

Uso

La Technical and Electronic Support Unit (TESU, Unidad de Soporte Técnico y Electrónico) administra y mantiene todos los sistemas de grabación de audio que utiliza el SPD. La TESU recibe solicitudes verbales para la implementación de esta tecnología por parte de los detectives del SPD que investigan delitos, documenta el equipo solicitado y el número de caso y guarda una copia de la orden judicial que autoriza el uso del equipo. Luego, la TESU brinda el equipo al oficial o detective solicitante para que lo utilice dentro del ámbito de aplicación del formulario de consentimiento o la orden judicial.

Protecciones

La implementación de los dispositivos de grabación de audio está restringida a las condiciones previstas por el consentimiento o la orden judicial, que proporcionan la autoridad legal y el ámbito de aplicación de los datos obtenidos. Los dispositivos de grabación de audio se utilizan solo después de que se hayan cumplido los estándares legales de consentimiento o una orden judicial emitida por un tribunal, como lo requiere la Washington Privacy Act, cap. 9.73 del RCW. Además, todas las implementaciones de los dispositivos de grabación de audio están documentadas por la TESU y están sujetas a auditoría por parte de la Office of Inspector General (Oficina del Inspector General) y el supervisor federal en cualquier momento.

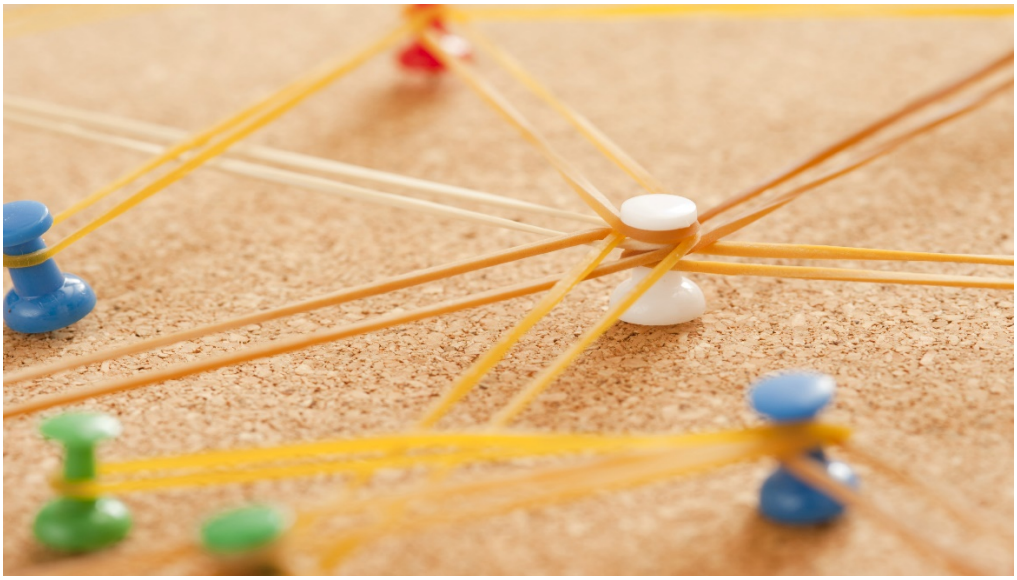
City of Seattle

Análisis de enlaces: IBM I2 iBase

Seattle Police Department (SPD)

¿En qué consiste esta tecnología?

La aplicación iBase permite a los usuarios combinar los datos almacenados en los sistemas de información penal del Seattle Police Department (SPD, Departamento de Policía de Seattle) con la información recopilada durante las investigaciones penales y exhibir esa información en un gráfico de enlaces. Este tipo de análisis de enlaces es similar a un "tablón de notas" virtual, que ayuda a los investigadores a visualizar las conexiones entre entidades conocidas, vehículos, ubicaciones, etc. en el curso de una investigación penal. El sistema de I2 iBase es compatible con el CJIS, y solo los usuarios autorizados pueden acceder al sistema, la tecnología o los datos.



Se encuentra abierto el período para recibir comentarios del público sobre esta tecnología. Puede enviar sus comentarios a **Seattle.gov/Surveillance**.

Todos los comentarios se incluirán en el "Informe del efecto de la vigilancia" sobre esta tecnología y se presentarán ante el Consejo.

Si le gustaría compartir comentarios fuera del período abierto para recibir comentarios del público, preséntelos directamente al Consejo de la ciudad.

¿Por qué usamos esta tecnología?

Antes de la implementación del software iBase, los investigadores debían volver a escribir toda la información penal del RMS en gráficos de visualización, lo que suponía un proceso lento y redundante. La implementación de iBase les permitió a los usuarios graficar esa información sin tener que volver a escribirla.

Obtención

La aplicación iBase importa de manera automática una parte de los datos en el Records Management System (RMS, sistema de gestión de registros) y el sistema de Computer Aided Dispatch (CAD, despacho asistido por computadora) del SPD. Los usuarios también pueden agregar de forma manual información adicional que hayan obtenido durante el curso de una investigación penal a fin de ayudar a comprender investigaciones complejas.

Uso

Los analistas utilizan en la actualidad IBM i2 iBase dentro del Real Time Crime Center (RTCC, Centro de Crímenes en Tiempo Real) a fin de ayudar con las investigaciones penales y brindar información útil a las unidades en el campo. Los empleados del SPD en el RTCC y la Unidad de Investigaciones utilizan el software i2 Analyst's Notebook para graficar la información almacenada en el sistema de i2 iBase. Los analistas crean visualizaciones que demuestran las conexiones entre entidades conocidas, vehículos, ubicaciones, etc. en el curso de las investigaciones penales.

Protecciones

Solo los usuarios autorizados pueden acceder al sistema, la tecnología o los datos. Para acceder al sistema de iBase, el personal del SPD debe iniciar sesión con credenciales de acceso protegidas con contraseña. Todos estos empleados están certificados por ACCESS y el Criminal Justice Information System (CJIS, Sistema de Información de Justicia Penal).
El sistema de I2 iBase es compatible con el CJIS. El software también registra el inicio o cierre de sesión del usuario cada vez que este accede a cualquier dato o realiza una adición o un cambio.

Análisis de enlaces: Maltego

Seattle Police Department (SPD)

¿En qué consiste esta tecnología?

Maltego de Paterva es una plataforma de Open Source Intelligence (OSINT, Inteligencia de Código Abierto) que presenta información disponible al público en un modelo visual de entidad-relación fácil de interpretar y permite a los investigadores analizar conexiones entre individuos relacionados con investigaciones penales. El uso de Maltego se rige por la política del SPD, la City of Seattle Intelligence Ordinance (Ordenanza de Inteligencia de la Ciudad de Seattle), el título 28, parte 23 del CFR y los requisitos del Criminal Justice Information System (CJIS, Sistema de Información de Justicia Penal).

Se encuentra abierto el período para recibir comentarios del público sobre esta tecnología. Puede enviar sus comentarios a **Seattle.gov/Surveillance**.

Todos los comentarios se incluirán en el "Informe del efecto de la vigilancia" sobre esta tecnología y se presentarán ante el Consejo.

Si le gustaría compartir comentarios fuera del período abierto para recibir comentarios del público, preséntelos directamente al Consejo de la ciudad.

¿Por qué usamos esta tecnología?

Maltego es una herramienta importante utilizada por el SPD en las investigaciones de delitos cibernéticos, ya que estos incidentes a menudo involucran interacciones entre personas, dispositivos y redes que de otro modo se desconocerían. Maltego consulta datos públicos en Internet, como dominios, y los exhibe en un diagrama que muestra los enlaces. Esta herramienta es utilizada por agentes policiales locales, así como en toda la comunidad de seguridad de la información, tanto para programas defensivos de seguridad cibernética como para investigar infracciones y casos de delitos cibernéticos.

Obtención

Maltego consulta datos disponibles al público en Internet y recopila información basada en los parámetros de la solicitud de búsqueda ingresados por un detective, al igual que Google produce resultados basados en términos de búsqueda específicos.

Uso

Maltego es una aplicación de software de seguridad cibernética que se utiliza para ayudar al Seattle Police Department (SPD, Departamento de Policía de Seattle) a investigar datos disponibles al público y diagramar asociaciones entre personas, dispositivos y redes, como parte de una investigación de delitos cibernéticos. SPD utiliza Maltego para investigar delitos cibernéticos, principalmente para determinar el origen digital de los ataques contra una infraestructura cibernética.

Protecciones

El uso de Maltego se rige por la política del SPD, la City of Seattle Intelligence Ordinance, el título 28, parte 23 del CFR y los requisitos del CJIS. El acceso a Maltego está restringido para usos relacionados con los incidentes de seguridad asociados o las investigaciones penales correspondientes y está sujeto a la política del departamento con respecto a las investigaciones penales en curso. Maltego es utilizado por dos detectives capacitados de la TESU dentro de la TESU, y por ninguna otra entidad.