Si un agente golpes

centerforconstitutionalrights

on the front lines for social justice

Índice

Introducción

Las agencias federales de las fuerzas del orden, como el Buró Federal de Investigación (FBI), tienen una historia oscura de persecución a movimientos radicales y progresistas. Algunos de los trucos sucios que usan contra estos movimientos incluyen: infiltración de organizaciones para desacreditar y desbaratar sus operaciones, campañas de información errónea e historias falsas en los medios de comunicación, falsificación de correspondencia, falsificación de pruebas y el uso de órdenes de comparecencia del Gran Jurado para intimidar a los activistas. El activista de hoy en día debe conocer y comprender la amenaza que representan los agentes federales de las fuerzas del orden y sus tácticas, al igual que varias prácticas de seguridad clave que ofrecen la mejor protección.

Los agentes federales tienen muchas herramientas a su disposición para perseguir a los activistas. Si bien es importante conocer y comprender estas herramientas y tácticas, es de fundamental importancia que evite todo tipo de paranoia con respecto a la vigilancia del gobierno o el temor a la infiltración, que sólo servirán para paralizarlo a usted o a la organización en su cruzada a favor del cambio social. Si el temor a la represión del gobierno le impide organizarse, los agentes de la represión habrán ganado sin siquiera hacer un esfuerzo.

El Centro para los derechos constitucionales (Center for Constitutional Rights, CCR) creó "If an Agent Knocks" (Si un agente llama a su puerta) para brindar asesoramiento a los activistas con probabilidades de ser perseguidos por agentes del FBI u otros investigadores federales. Desde su lanzamiento original en 1989, Si un agente llama a su puerta se ha divulgado ampliamente entre comunidades activistas progresistas de todo el país. Esta guía incluye tanto los consejos que nunca caducan incluidos en la versión original

así como amplias actualizaciones que reflejan el estado actual de la ley y de las herramientas de imposición del cumplimiento de la ley. Esta edición actualizada incluye además un comentario completo sobre la tecnología actual, incluyendo teléfonos celulares, correo electrónico y navegación por Internet. Esta guía debe verse como un recurso con la información necesaria para protegerse usted y proteger a otros activistas contra investigaciones del gobierno, y para darle el poder de seguir con la lucha.

Hemos intentado responder una amplia gama de preguntas sobre los varios escenarios con lo que tal vez se enfrente en su calidad de activista. Esperamos que tanto las personas como los grupos usen este panfleto para desarrollar y preparar respuestas prácticas, si un agente llama a su puerta.

Esta publicación hace énfasis, sistemáticamente, en la necesidad de procurar asesoramiento legal profesional en todos los casos. El Centro para los derechos constitucionales no cuenta con la capacidad de proporcionar representación penal individual.

Cada estado tiene asociaciones jurídicas con la capacidad de recomendar abogados, algunos de los cuales tal vez ofrezcan servicios gratuitos. Si hubiera una sección de la Asociación nacional de abogados (National Lawyers Guild, www.nlg.org) en su ciudad, por lo general pueden recomendarle abogados con experiencia en manejar los problemas detallados en este folleto.

Visitas y búsquedas

Esta es la información más importante de este folleto: tiene derecho a guardar silencio, y por lo general, hacerlo es la mejor idea. La Quinta Enmienda de la Constitución de los Estados Unidos lo protege en caso de que lo obliguen a revelar información que lo incrimine a los agentes de las fuerzas del orden.

Esto es más fácil de decir que de hacer. Los agentes son investigadores entrenados: han aprendido el poder de persuasión y adquirido la capacidad de hacer que una persona se sienta asustada, culpable o grosera por negarse a satisfacer sus pedidos de información.

Es posible que un agente sugiera que el hecho de no querer hablarle significa que tiene usted algo que ocultar. Puede que sugiera que sólo quiere que le responda unas preguntas y que luego lo dejará tranquilo. Es posible que el agente amenace con obtener una orden judicial.

No se deje intimidar ni manipular por las amenazas o afirmaciones de un agente.

Si se me acerca o me llama un Agente de las fuerzas del orden, ¿tengo que hablar?

Siempre es mejor no hablar sin un abogado presente. Si habla, todo lo que diga podrá ser utilizado en contra suya y de otros. Incluso si dice toda la verdad, si el agente no le cree, puede amenazarlo con la acusación de mentirle a un oficial federal, lo que consiste un delito real.

Transmita claramente su intención de guardar silencio. Diga “No voy a hablar con usted” o “Me gustaría hablar con mi abogado antes de decirle algo a usted”. También puede decir “No tengo nada que decirle.

Hablaré con mi abogado y él se

comunicará con usted". Debe pedir al agente una tarjeta y decir que su abogado lo llamará. Esto debería dar por terminado el interrogatorio.

La única excepción a esta regla es que usted se encuentre en un estado que cuenta con un estatuto de "detención e identificación". Todos los estados exigen que muestre su licencia de conducir si le piden que se detenga mientras va conduciendo un auto, y la Corte Suprema ha sostenido que las leyes que le exigen dar su información básica de identificación, como por ejemplo su nombre y su dirección, no se consideran incriminatorias, y que los agentes de la fuerza del orden pueden exigirle dicha información.

Sin embargo, solamente pueden exigirle esa información si usted está en un estado que cuenta con un estatuto de detención e identificación. Un abogado activista de su estado podrá decirle si existe tal estatuto en su estado.

Las mismas reglas básicas se aplican si un agente llama por teléfono. Usted no está obligado a hablar con ningún agente que lo llame espontáneamente. A menudo los agentes le dirán que usted no es parte de ninguna investigación. Esto puede no ser cierto. Dígale a cualquier persona que se identifique como agente de las fuerzas del orden que su abogado lo llamará, y deje de hablarle.

Si fuera posible, obtenga el nombre del agente, su teléfono y su agencia. Estos deberían estar en su tarjeta personal, o de lo contrario debería estar dispuesto a darle esta información.

En cuanto el agente se vaya o cuelgue el teléfono, intente anotar tantos detalles sobre la interacción como sea posible. Esta información será útil para un abogado y para otras personas que hayan sido contactadas por agencias de fuerzas del orden.

Intente anotar el nombre del o de los agentes y su descripción física, el tipo de auto que el agente conducía, las preguntas que le hizo y los comentarios efectuados durante la interacción, la fecha, hora y lugar del encuentro, y la información de contacto de cualquier testigo.

El mejor curso de acción suele ser dar participación a un abogado. Un abogado puede ofrecer consejos sobre cómo proceder mientras protege sus derechos. Un abogado puede hablar con el agente; averiguar de qué se trata la investigación, intentar poner límites al tema de cualquier interrogatorio, y estar presente para aconsejarlo y protegerlo si lo interrogan. A veces, la llamada de un abogado es todo lo que se necesita para lograr que un agente dé un paso atrás.
Con el asesoramiento de un abogado, tal vez pueda tener en

cuenta revelar el encuentro a otras personas que podrían resultar afectadas por una investigación. Si los activistas saben que hay una investigación, pueden estar más atentos en cuanto a la protección de sus derechos. La organización y la presión pública pueden dejar en evidencia y limitar la intimidación y las expediciones de "pesca".

¿Cuáles son las consecuencias si hablo?

Tal vez surja una situación en la que considere que es aconsejable hablar con un agente. Quizá haya sido usted víctima de un crimen, o testigo de violaciones de los derechos civiles llevadas a juicio por el gobierno federal.

Incluso en esos casos, debería tener un abogado presente. Un abogado puede asegurarse de que sus derechos sean protegidos mientras usted proporciona sólo la información necesaria relevante para un incidente específico. Posiblemente lo ayude a evitar una comparecencia como testigo ante un gran jurado o a controlar las circunstancias de la comparecencia, de modo tal de no poner los derechos de nadie en peligro.
Si decide responder preguntas, tenga en cuenta que es delito mentirle a un funcionario del gobierno. De hecho, uno de los motivos más importantes para no hablar con un agente es este delito. Una táctica estándar de las agencias federales de la fuerza del orden es descubrir tanta información como sea posible acerca de un sospechoso, o simplemente de una persona que reviste interés para el gobierno. Los agentes federales de las fuerzas del orden se acercarán entonces a dicha persona, en un momento cualquiera, como por ejemplo durante la cena o en la parada del autobús, y harán preguntas a esa persona de las que ya saben la respuesta.

Por ejemplo, un agente podría preguntarle si conoce a alguien (a quien ya saben que usted conoce), o tal vez si asistió a un evento (al que saben que usted asistió). Si usted responde "No" por instinto, eso es un delito federal grave penado con cinco a ocho años de prisión. El aspecto más desalentador de esta táctica de investigación es que muchas personas instintivamente responderán que no a una pregunta porque se asustan o se ponen nerviosas. Esta táctica es muy utilizada por agentes federales en todo tipo de investigaciones, y se ha usado recientemente para

1. En el momento de la publicación, los estados que cuentan con alguna versión de estatuto de detención e identificación son los siguientes: Alabama, Arizona, Arkansas, Colorado, Delaware, Florida, Georgia, Illinois, Indiana, Kansas, Louisiana, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Rhode Island, Utah, Vermont y Wisconsin.

localizar activistas y convertirlos en informantes, poniéndolos en contra de sus antiguos colegas.

Mentir a un funcionario federal es una ofensa federal que sólo se aplica a las preguntas formuladas por agentes federales. No obstante, tenga presente que algunos agentes locales y estatales, como por ejemplo los miembros del Grupo de trabajo unido contra el terrorismo de un municipio, también se consideran agentes “federales”. Además, algunos estados tienen delitos similares relativos a mentirle a un funcionario del estado. La opción más segura es no hablar con los agentes de las fuerzas del orden. Si comienza a responder preguntas, puede rehusarse a seguir respondiendo en cualquier momento.

Órdenes de allanamiento

Una orden de allanamiento es una orden judicial que autoriza a las fuerzas del orden a revisar un lugar específico para obtener evidencias.

La Cuarta Enmienda protege a las personas contra búsquedas poco razonables. Salvo que se aplique una excepción, los agentes de las fuerzas del orden tienen la obligación de obtener una orden de allanamiento para llevar a cabo una revisión. Las órdenes de allanamiento deben estar respaldadas por una causa probable, con hechos que haya declarado bajo juramento el funcionario que solicita la orden. Una orden de allanamiento debe especificar el área a revisar y el o los objetos que se buscan. Debe estar firmada por un juez, tener una fecha reciente (no más de un par de semanas de antigüedad) y determinar la dirección correcta del lugar.

"Causa probable" significa que deben existir hechos que establezcan que es probable encontrar evidencias de un delito en el área a revisar. La causa probable debe basarse en hechos; los presentimientos no son suficientes. Armados con una orden de allanamiento, los agentes de las fuerzas del orden tienen derecho a revisar su propiedad.

Si no les permite acceder, es probable que lleven a cabo la revisión por la fuerza.

Conozca las herramientas de ellos

¿Qué pasa si un agente me pide revisar mi casa, mi apartamento o mi oficina?

Jamás permita a las fuerzas del orden revisarlo, o revisar su propiedad, sin una orden de allanamiento. Los agentes de las fuerzas del orden tienen la obligación de tener una orden de allanamiento para revisar su propiedad, salvo en determinadas circunstancias limitadas. La ley sólo lo obliga a permitir que los agentes de la fuerza del orden entren en su casa, oficina u otro espacio privado si tienen una orden de allanamiento.

Los agentes podrán revisar su casa sin una orden si usted lo permite, y están entrenados para obtener su consentimiento para realizar revisiones sin orden de allanamiento. Tenga cuidado con las preguntas diseñadas para sacarle el consentimiento para revisar. Estas preguntas podrían ser tan inocuas como "¿Puedo pasar?". El simple permiso a un agente para ingresar en su hogar podría interpretarse como un consentimiento para revisar todo el lugar.

Legalmente, la mejor respuesta ante una solicitud de revisión es "No acepto que se haga una revisión". Dígalo en voz alta y con orgullo, para que lo escuche

cualquier testigo.

¿Qué pasa si no estoy en casa y un agente le pide a mi compañero de casa para revisar mis cosas?

Un compañero de casa puede consentir la revisión del espacio común compartido y de su propio espacio. Pero no puede consentir la revisión del espacio privado de otra persona en una casa o apartamento compartido. Dicho de otra forma, un compañero de casa puede consentir que revisen su cocina, su sala o el baño compartido, pero no su dormitorio personal, salvo que lo comparta con él o que se use como espacio común de alguna manera.

Los cónyuges pueden consentir la revisión de las habitaciones privadas de su pareja porque se considera que comparten la autoridad sobre todos los espacios de la casa. De manera similar, los padres pueden permitir la revisión del espacio privado de sus hijos. En resumen, si comparte el dormitorio con un compañero o su pareja, ellos podrán permitir una revisión de dicho espacio.

Para protegerse contra revisiones no deseadas, asegúrese de que el espacio privado se mantenga privado. Si permite a sus

compañeros de casa que accedan y controlen su espacio privado, podrán dar su consentimiento para la revisión de ese espacio. Diga a sus compañeros de casa, compañeros de oficina y a todos quienes compartan un espacio con usted que jamás acepten que se revise ningún espacio, en especial su espacio personal.

¿Los agentes pueden revisar mi basura?

Una vez que haya colocado su basura afuera de su casa, los agentes pueden revisarla sin una orden de allanamiento ni ninguna otra restricción legal. Los tribunales han determinado que no

existe interés de privacidad en su basura, porque la está sometiendo al público en general. Triture o destruya de otra manera todos los documentos delicados antes de desecharlos.

¿Qué pasa si un agente amenaza con obtener una orden de allanamiento, o una citación del Gran Jurado, salvo que hable o acepte que me revisen?

No se deje intimidar por las amenazas de un agente de obtener una orden de allanamiento o una orden de comparecencia. Este es uno de los trucos más viejos del manual. Si fuera tan fácil para el agente obtener una orden de allanamiento o una orden de comparecencia, no habría perdido tiempo intentando obtener su colaboración voluntaria. Una vez más, sencillamente dígale que no aceptará ninguna revisión y que no hablará sin la presencia de un abogado.

¿Qué pasa si un agente manifiesta tener una orden de allanamiento?

Si un agente manifiesta tener una orden de allanamiento, pídale que se la muestre. Debe verse parecida a la muestra de orden de allanamiento que presentamos aquí, y para ser válida debe estar firmada por un juez. Una orden de allanamiento debe especificar el área a revisar y el o los objetos que se van a buscar. No permita que un agente revise áreas que no estén específicamente incluidas en una orden de allanamiento.

Sólo porque un agente tenga una orden de allanamiento usted no está obligado a responder ninguna pregunta. Durante la revisión, conserve su derecho a guardar silencio; manifieste claramente esa intención si le hacen alguna pregunta.

¿Qué derechos tengo para impedir que los agentes revisen mi auto?

Las fuerzas del orden tienen un poder sumamente amplio para revisar autos sin órdenes de allanamiento. Si un agente tiene causa probable para creer que un auto contiene evidencia

de un delito, el agente podrá, sin orden de allanamiento, revisar el vehículo y cualquier recipiente dentro del mismo que sea lo suficientemente grande como para contener el elemento que se está buscando con causa probable. Por ejemplo, si un agente tiene causa probable para creer que usted robó un televisor grande, podrá revisar la cajuela del auto, pero no la guantera ni una cajita de herramientas que haya en la cajuela. Si sólo tiene causa probable para buscar en un recipiente recientemente colocado en el auto, sólo podrá buscar en ese recipiente.

Si lo arrestan y su auto es llevado al depósito municipal, las fuerzas del orden pueden realizar una revisión de inventario sin orden de allanamiento. Básicamente, esto quiere decir que la policía podrá revisar su auto para catalogar lo que hay adentro, pero podrán usar contra usted cualquier cosa que encuentren, por el motivo que sea. Las revisiones de inventario deben seguir los procedimientos locales dispuestos, y la policía no podrá usar una revisión de inventario como pretexto para realizar una revisión sin orden de allanamiento.

Revisiones furtivas

Las revisiones furtivas permiten al gobierno, con la aprobación secreta de un tribunal, realizar búsquedas y vigilancias sin notificar al sujeto de la investigación. Como se supone que las revisiones furtivas se realicen en secreto, suelen ser llevadas adelante mediante entrada forzosa.

Normalmente, un agente debe comparecer ante un juez y demostrar causa probable a fin de obtener una orden de allanamiento. No obstante, en el Tribunal de vigilancia de inteligencia extranjera, los agentes pueden obtener una autorización para llevar a cabo una revisión furtiva, si pueden demostrar que dicha revisión proporcionará información de inteligencia extranjera. Y la recolección de inteligencia extranjera no tiene que ser el motivo principal de la revisión; simplemente debe ser un motivo relevante de la revisión. Esto quiere decir que un agente puede obtener autorización para revisar su casa en busca de evidencias de actos delictivos siempre y cuando también tenga el objetivo de reunir información de inteligencia extranjera durante la revisión.

Si bien las revisiones furtivas fueron diseñadas con el fin de reunir información de inteligencia extranjera, la mayoría de los tribunales han admitido el uso de evidencias e información obtenidas a partir de revisiones furtivas en procesos penales.

Conozca las herramientas de ellos

¿Qué debo hacer si entran a la fuerza en mi oficina o en mi casa, y sospecho que el motivo fue la obtención de información?

Si entran a la fuerza en su casa u oficina, o si lo han amenazado a usted, a su organización o a alguien que trabaja con usted, comparta esta información de inmediato con todos los afectados, y tome medidas inmediatas para aumentar la seguridad personal y de la oficina. Póngase en contacto de inmediato con un abogado.

¿Qué debo hacer si los agentes se presentan con una orden de arresto?

Una orden de arresto es una herramienta empleada por la policía y otras agencias de las fuerzas del orden para entrar en su casa y realizar un arresto.

Uno de los muchos vacíos legales de los requisitos de las órdenes de allanamiento es que una vez que los agentes están dentro de su hogar, aunque estén allí sólo con una orden de arresto, tienen gran libertad de acción para llevar a cabo una revisión. Pueden revisar el área circundante inmediata sin

Orden de arresto

Una orden de arresto es una orden judicial que autoriza a las fuerzas del orden a arrestar a una persona específica. Las órdenes de arresto están firmadas y emitidas por un juez sobre la base de solicitudes bajo juramento de las fuerzas del orden de que hay causa probable de que se haya cometido un delito, y de que la o las personas nombradas en la orden cometieron el delito.

En general, la policía y demás agentes de las fuerzas del orden no necesitan una orden para hacer un arresto. Si tienen causa probable para creer que se ha cometido un delito, pueden hacer un arresto.

Esta regla tiene dos excepciones comunes. La primera, en la mayoría de los estados, los agentes de las fuerzas del orden necesitan una orden para hacer un arresto por un delito menor que no presenciaron personalmente. No obstante, es importante tener en cuenta que los agentes igual pueden hacer arrestos por delitos graves de los que no fueron testigos sin una orden de arresto. En segundo lugar, las fuerzas del orden por lo general necesitan una orden de arresto para arrestarlo en su casa. Sin embargo, pueden hacer un arresto sin orden en su hogar si creen que existe un riesgo de que destruya evidencia o si están tras usted en encarnizada persecución y usted se esconde en la casa de un tercero.

Conozca las herramientas de ellos

una orden de allanamiento.

Los agentes de las fuerzas del orden incluso pueden revisar toda la casa como parte de un "barrido de protección" si tienen sospechas razonables de que allí pueda haber una persona peligrosa.

Si las fuerzas del orden llegan a su casa (o a cualquier otro sitio) con una orden de arresto, lo mejor que puede hacer es salir y entregarse. Si es seguro hacerlo, tranque la puerta al salir. Si los agentes de las fuerzas del orden tienen una orden de arresto, lo arrestarán. No les dé la oportunidad de realizar además una revisión de su casa sin orden de allanamiento.

Órdenes de comparecencia

Una orden de comparecencia es una orden emitida por una autoridad gubernamental que exige que alguien entregue una prueba material, como por ejemplo documentos, o que la persona atestigüe ante un tribunal.

Es sumamente sencillo obtener una orden de comparecencia. Suelen ser solicitadas por un funcionario del gobierno, un actuario e incluso por abogados particulares. No es necesario presentar una orden de comparecencia ante un juez antes de emitirla. La evidencia requerida para emitir una orden de comparecencia es sumamente sencilla; se puede emitir una orden de comparecencia si existe una posibilidad razonable de que la prueba material o el testimonio solicitados proporcionen información relevante al asunto que se está investigando.

La sencillez con la cual se emiten las órdenes de comparecencia las transforma en una herramienta poderosa, pero a diferencia de las órdenes de allanamiento u otras herramientas del gobierno, pueden recusarse ante un tribunal antes de su cumplimiento. Si recibe una orden de comparecencia, puede proceder a anular dicha orden si fuera demasiado amplia u onerosa, o si buscara obtener materiales protegidos por ley, incluyendo materiales protegidos por la Primera Enmienda. Una vez anulada la orden de comparecencia, el receptor de la orden ya no deberá presentar los documentos o el testimonio exigidos.

Las órdenes de comparecencia son particularmente peligrosas, porque las fuerzas del orden pueden presentar órdenes de comparecencia a terceros que tal vez tengan información sobre usted. El gobierno puede ordenar la comparecencia de otras personas por correos electrónicos que usted les haya enviado. O pueden pedir esos correos electrónicos a su servidor de correo. Porque estos terceros no tienen el mismo interés de rechazar estas órdenes que usted, y es más probable que cumplan con la orden sin resistirse.

Conozca las herramientas de ellos

¿Qué debo hacer si recibo una orden de comparecencia?

Debe procurar anular la orden de comparecencia antes de la fecha de cumplimiento especificada en la orden misma, pero ni siquiera las órdenes de comparecencia que exigen un cumplimiento inmediato pueden hacerse cumplir sin la intervención de un juez.

Si alguien aparece en su puerta e intenta entregarle una orden de comparecencia, tómela. No deje entrar a la persona, no responda ninguna pregunta y no permita que lo revisen. Una orden de comparecencia no da al agente el derecho de tomar medidas inmediatas.

A fin de obtener ayuda para anular la orden de comparecencia, debe procurar los servicios de un abogado.

En el caso improbable de que le informen que un tercero ha recibido una orden de comparecencia por registros sobre usted, puede proceder a anular esa orden de comparecencia; no importa si una orden no fue emitida directamente para usted.

Infiltración y vigilancia de personas

El uso de agentes encubiertos e informantes es indispensable en las investigaciones realizadas por agencias modernas de las fuerzas del orden. La capacidad de ubicar agentes encubiertos o informantes en movimientos u organizaciones progresistas ofrece a las fuerzas del orden un tipo de acceso que de otro modo les resultaría imposible obtener.

La infiltración es muy útil para reunir información confidencial sobre las actividades de personas particulares y proporcionar a las fuerzas del orden información suficiente para iniciar una investigación. Los agentes encubiertos e informantes pueden reportar a las fuerzas del orden sobre los participantes, tácticas y acciones de los movimientos. Incluso pueden sugerir, fomentar y/o participar en actividades ilegales en su esfuerzo por arrestar participantes. Los tribunales en general han sostenido que las normas públicas prohíben la divulgación del nombre de un informante salvo que sea fundamental para la defensa en un tribunal penal, por lo que los informantes rara vez son convocados a testificar; esto les permite actuar con sólo una cantidad limitada de responsabilidad.

Informantes

Los informantes son personas que no trabajan como agentes de las fuerzas del orden y proporcionan información a dichos agentes, por lo general a cambio de dinero. Un informante suele haber estado involucrado previamente en el movimiento o en la organización que los agentes están investigando, y tienen un conocimiento íntimo del mismo.

⚠ Conozca las herramientas de ellos

Agentes encubiertos

Un agente encubierto es un funcionario de las fuerzas del orden que utiliza un nombre ficticio o una identidad falsa para infiltrarse en un movimiento u organización, con el fin de reunir información o pruebas. En casos de infiltración política, un agente típicamente se mostrará como simpatizante de una organización en particular, se ganará la confianza de los miembros clave y luego usará este acceso para reunir información confidencial que entregará a la agencia de investigación. Un objetivo secundario puede ser establecer las bases para otra investigación. Los agentes encubiertos típicamente inventan una historia falsa con tanto detalle como la misión requiera, al igual que una historia biográfica básica y creíble que abarque actividades anteriores y actuales.

⚠ Conozca las herramientas de ellos

Testigos colaboradores

Los testigos colaboradores son similares a los informantes, salvo que por lo general aceptan "darse vuelta" o "ir con el cuento" luego de ser amenazados con ser procesados. Los testigos colaboradores testificarán ante un tribunal a cambio de una reducción de los cargos en su contra, si los hubiera.

Las fuerzas del orden reclutan informantes y testigos colaboradores entre las filas de las personas ya activas dentro de los movimientos u organizaciones que se persiguen. El gobierno suele amenazar a estas personas con presentar cargos que implican un tiempo en la cárcel, y ofrecen no presentar cargos a cambio de una promesa de informar sobre otros miembros del movimiento. Los agentes encubiertos, por otra parte, actúan de manera falsa desde el principio de su vinculación con cualquier movimiento u organización.

⚠ Conozca las herramientas de ellos

Lo que los agentes encubiertos e informantes pueden hacer, ¿tiene límites?

No hay ninguna ley que rija o limite el uso de agentes encubiertos o informantes por parte de las fuerzas del orden, ni hay tampoco restricciones en el tipo de delito para los que se puede usar la infiltración con fines de investigación.

A diferencia de otros países, el uso de prácticas encubiertas no requiere una orden judicial, por lo que los funcionarios de las fuerzas del orden no necesitan demostrar la necesidad del uso

de un agente encubierto o de un informante para una investigación en particular. El uso de agentes encubiertos e informantes por parte del FBI está regido únicamente por pautas internas poco precisas, dispuestas en virtud de las conclusiones del Congreso de los EE.UU. en el Informe del Comité selecto para el estudio de las operaciones del gobierno con respecto a actividades de inteligencia (Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities) de 1976.

El informe expuso detalles sobre el ahora infame Programa de Contrainteligencia (COIN-TELPRO) del FBI, en funcionamiento entre 1956 y 1971, que persiguió a activistas y organizaciones, incluyendo al Dr. Martin Luther King Jr. y al partido de las Panteras negras.
En respuesta al informe, el Fiscal General de los EE.UU. aprobó pautas internas para las operaciones encubiertas del FBI, que regulaban tanto a los agentes encubiertos como a los informantes. Si bien estas pautas eran sólidas en un principio, se han ido debilitando progresivamente durante varias administraciones.

Las pautas actuales admiten muchas de las prácticas invasivas de cumplimiento de la ley que originalmente buscaban impedir. Es más, las pautas no pueden hacerse cumplir por orden de un tribunal, por lo que sólo ofrecen una protección limitada contra la infiltración y la vigilancia. Dicho de otro modo, si un agente reúne evidencia contraviniendo las reglamentaciones del FBI, dicha evidencia igual podrá ser usada en un tribunal.

¿Qué es la inducción a la comisión de un delito?

La mayor restricción sobre los agentes encubiertos y los informantes es el requisito de evitar inducir a cometer un delito. La inducción a la comisión de un delito ocurre cuando un agente o un informante planta la idea de cometer un delito en la mente de una persona que, de otro modo, no hubiera estado dispuesto a hacerlo, y luego alienta a dicha persona a cometer el delito con el fin de procesarlo posteriormente. Los tribunales ven a los casos de inducción a la comisión de un delito de manera muy limitada, y tienden a dar una gran flexibilidad a los agentes encubiertos o a los informantes que sugieren o fomentan actividades ilegales. Si bien las excepciones a la defensa por inducción a la comisión de un delito varían de un estado a otro, por lo general no es una defensa efectiva si el agente encubierto simplemente sugiere que se cometa

¿Qué es la inducción a la comisión de un delito? (continuación)

un crimen. En muchos estados, la inducción a la comisión de un delito no es una defensa viable si un jurado cree que alguien estaba predispuesto a cometer el delito.

¿Cuáles son los límites constitucionales del poder de un agente para infiltrarse?

Los agentes encubiertos o los informantes por lo general tienen permitido asistir a reuniones públicas, incluyendo las que se llevan a cabo en lugares de culto. Los tribunales a veces encontraron violaciones a la Primera Enmienda cuando se determina que los agentes de las fuerzas del orden interfirieron con la capacidad de un grupo de ejercer el derecho a la libertad de expresión y de asociación. De manera similar, algunos tribunales han encontrado que las fuerzas del orden violaron la Primera Enmienda al reunir y divulgar públicamente información sobre un activista o una organización. Los tribunales no han encontrado violaciones a la Primera Enmienda en casos donde los agentes de las fuerzas del orden simplemente generaron un ambiente incómodo en reuniones públicas.

Los tribunales han encontrado, sistemáticamente, que la grabación encubierta de conversaciones por parte de agentes encubiertos e informantes no viola la Cuarta Enmienda, que protege contra revisiones y confiscaciones poco razonables.

Los tribunales han encontrado, además, que la grabación encubierta de conversaciones por parte de agentes encubiertos e informantes no viola la protección de la Quinta Enmienda contra la autoincriminación. De manera similar, si usted, sin saberlo, invita a un agente encubierto a su casa o a otro lugar privado, los tribunales considerarán esto como un “consentimiento” para que el agente realice una revisión. Si el agente encubierto percibiera una causa probable de delito, podrá entonces convocar a otros agentes de las fuerzas del orden para que se unan a él en la búsqueda basándose en el supuesto consentimiento otorgado al agente encubierto. Algunos tribunales incluso han aplicado el mismo razonamiento para las situaciones en las que el blanco mismo invita sin saber al informante a entrar en una casa.

¿Cómo puedo determinar evidencias de infiltración?

Hay algunas pistas útiles para identificar a un infiltrado. Es probable que un agente encubierto o un informante se ofrezcan como voluntarios para tareas que ofrezcan acceso a las reuniones y documentos importantes de su grupo, tales como registros financieros, listas de miembros, actas y archivos confidenciales. Los agentes encubiertos e informantes a menudo fomentan o incitan al uso de violencia o tácticas ilegales, y acusan de cobardes a quienes se resisten a implementar esas tácticas. De manera similar, los agentes encubiertos o informantes a menudo acusan a otros de ser agentes o informantes, desviando la atención de sí mismos y distrayendo al grupo de su trabajo. Un agente encubierto o informante tal vez no tenga una fuente de ingresos obvia durante un período de tiempo, o tenga más dinero disponible de lo que su trabajo le proporcionaría.

Intente obtener información sobre los antecedentes de un supuesto agente o informante. Verifique con las organizaciones de áreas donde el supuesto agente vivió anteriormente, para ver si hay alguien que responda por él. Vea lo que puede encontrar en Internet. Los registros públicos tales como informes de crédito, registro de votantes e hipotecas contienen mucha información, incluyendo direcciones anteriores y la actual. Si están disponibles, tal vez desee verificar las listas de los graduados de la academia de policía local; pero recuerde: la persona de la que sospecha tal vez no esté usando su nombre verdadero.

Una persona que reúna todas estas características no es necesariamente un agente encubierto ni un informante. Tenga cuidado y no acuse a alguien de ser un agente o un informante salvo que tenga pruebas contundentes contra la persona.

¿Qué precauciones puedo tomar para proteger a mi organización?

Mantenga un archivo de todas las experiencias supuestas o confirmadas de vigilancia o interferencia. Incluya la fecha, el lugar, la hora, las personas presentes, una descripción completa de todo lo sucedido y cualquier comentario que explique el contexto de la experiencia y una descripción del impacto que tuvo el evento en la persona o en la organización. Haga una reunión para hablar sobre espionaje y acoso, y determine si alguno de sus miembros sufrió algún tipo de acoso, o percibió algún tipo

¿Qué precauciones puedo tomar para proteger a mi organización? (continuación)

de vigilancia aparentemente centrada en las actividades de la organización. Revise las actividades o los problemas pasados de su grupo que sean sospechosos, e intente determinar si hubo una o varias personas involucradas en muchos de estos hechos.

Puede intentar presentar solicitudes de la Ley de libertad de información (Freedom of Information Act, FOIA por sus siglas en inglés) para su organización en agencias tales como el FBI, el Departamento de seguridad interna (Department of Homeland Security, DHS por sus siglas en inglés), el Buró de alcohol, tabaco y armas de fuego (Bureau of Alcohol, Tobacco and Firearms) y demás agencias federales. Presente solicitudes similares en agencias de las fuerzas del orden locales y estatales utilizando las leyes de libertad de información de su estado.

Lo más importante es no permitir que la paranoia con respecto a la infiltración paralice a su movimiento u organización. La paranoia puede ser tan destructiva como la infiltración misma.

Vigilancia electrónica

Este capítulo trata de las formas en las que los agentes pueden usar escuchas telefónicas, micrófonos ocultos y vigilancia de Internet en sus investigaciones. A medida que nuestras vidas se tornan cada vez más digitalizadas, los agentes cada vez más usan la vigilancia electrónica para obtener información. Lamentablemente, la ley y los tribunales no suelen lograr seguirle el ritmo a la tecnología, lo cual a menudo conduce a un desconocimiento o una disminución de la protección de la privacidad ante las más recientes tecnologías.

Una buena regla general es la siguiente: cuanto más antiguo el medio de comunicación, más protección le brinda la ley. Tal como dijo Elliot Spitzer cuando era el Fiscal General del estado de Nueva York: “Nunca escriba cuando pueda hablar. Nunca hable cuando pueda asentir. Y nunca ponga nada en un correo electrónico, porque es la muerte. Estará dando a la acusación toda la evidencia que necesitamos”.

Comunicaciones telefónicas

Las conversaciones telefónicas pueden ser interceptadas de varias maneras: desde escuchas a micrófonos ocultos, y desde escuchas ambulantes hasta registros de llamadas salientes y dispositivos de control y rastreo. Los métodos de vigilancia telefónica son detallados y complejos, y aquí sólo podemos ofrecer un panorama general de ellos. La lección, no obstante, es sencilla: tenga mucho cuidado con lo que dice por teléfono.

¿Cuándo puede el gobierno intervenir mis teléfonos?

En general, el gobierno requiere de una orden judicial especial, llamada Orden de escucha del Título III, para escuchar sus conversaciones telefónicas. Sin embargo, el gobierno también puede escuchar su teléfono sin una garantía, durante 48 horas, en determinadas situaciones de emergencia relacionadas con la muerte o con lesiones graves inmediatas, con la seguridad nacional o con actividades características del crimen organizado.

Órdenes de escucha del Título III

Las órdenes de escucha del Título III son las órdenes judiciales utilizadas para interceptar y controlar sus comunicaciones. Además de las protecciones de la Cuarta Enmienda, que exigen órdenes de allanamiento para la mayoría de las revisiones, el Congreso otorgó protecciones adicionales acerca de la comunicación oral en el Título II de la Ley amplia del control del delito y la seguridad en las calles (Omnibus Crime Control and Safe Streets Act) de 1968. Estas protecciones aumentadas se aprobaron en respuesta a las conclusiones del Congreso con respecto a la generalización de la vigilancia ilegal y abusiva del FBI durante la década del 60 (véase "Lo que los agentes encubiertos e informantes pueden hacer, ¿tiene límites?").

Los agentes deben presentar una larga y pesada solicitud del Título III que incluye: hechos acerca del delito cometido o a punto de cometerse, el lugar desde donde se interceptarán las comunicaciones, las comunicaciones que se pretende interceptar, si se han utilizado otras herramientas de investigación que resultaron inadecuadas, o si otras herramientas resultarían inadecuadas o demasiado peligrosas de aplicar, el marco de tiempo en el que se llevarán a cabo las interceptaciones y una declaración de todas las aplicaciones anteriores de escuchas telefónicas acerca del mismo objetivo o en las mismas instalaciones.

Para emitir una Orden de escucha del Título III, un juez debe encontrar: causa probable de que el objetivo está cometiendo un delito incluido en el Título III, que mediante la intercepción se obtendrá la comunicación con respecto a ese delito y que las instalaciones desde donde se interceptará la comunicación se utilizarán en relación con el delito.

Originalmente, el Título III sólo admitía la vigilancia en una categoría

Conozca las herramientas de ellos

Órdenes de escucha del Título III (cont.)

específica de delitos graves. Con el correr de los años, el Congreso agregó más y más delitos a la cobertura del Título III. Hoy en día, la ley cubre cientos de delitos, incluyendo categorías más amplias como por ejemplo delitos relacionados con drogas, disturbios, obscenidad o interferencia con el comercio. Tales interpretaciones amplias de estos delitos admiten la vigilancia de muchas formas de activismo.

Las órdenes de escucha del Título III en principio pueden durar hasta 30 días. Las fuerzas del orden pueden recurrir nuevamente al juez para obtener extensiones reiteradas de 30 días. Una vez que vence una Orden de escucha del Título III, el juez puede ordenar al gobierno divulgar un inventario de las comunicaciones interceptadas a los objetivos de la escucha. Un inventario tal informa los objetivos del período que abarca la escucha y si efectivamente se interceptaron comunicaciones. No obstante, el juez puede optar por no solicitar la emisión de un inventario tal.

Generalmente, es una práctica poco frecuente que las fuerzas del orden soliciten órdenes judiciales para escuchas telefónicas, pero cuando lo hacen, casi siempre las consiguen. Por ejemplo, durante 2007 se presentaron sólo 2208 solicitudes de órdenes judiciales para escuchas telefónicas en tribunales estatales y federales, pero cada una de las solicitudes fue aprobada ese año. La amplia mayoría de las órdenes judiciales para escuchas telefónicas estuvieron relacionadas con casos de drogas (1729 de 2208, o el 81%), seguidos por casos de homicidio y agresión (132 de 2208, o el 6%).

Conozca las herramientas de ellos

¿Cómo sabré si mi teléfono está siendo intervenido?

Lo más probable es que no sepa si su teléfono está intervenido. La vigilancia del gobierno ha avanzado mucho desde la época en la que un clic, un pitido, un zumbido o cualquier otro sonido le daban indicios de una escucha telefónica. El gobierno, en general, debería informarle sobre la vigilancia dentro de los 90 días posteriores a la finalización de la misma, pero la notificación puede posponerse con relativa facilidad.

¿Qué es una escucha telefónica ambulante?

Típicamente, una escucha telefónica se aplica a un teléfono específico de un lugar específico luego de haber sido autorizada mediante una orden judicial. Sin embargo, una escucha telefónica ambulante es una escucha de cualquier teléfono, desde cualquier lugar donde el agente de las fuerzas del orden considere que el objetivo realizará llamadas telefónicas. La realización de escuchas telefónicas ambulantes por parte del gobierno se ha autorizado desde 1998. El gobierno necesita cumplir con los mismos estándares para una escucha ambulante que para una escucha común: causa probable de que se haya cometido o se esté por cometer un delito.

¿Qué hay de los micrófonos ocultos?

Un micrófono oculto es un dispositivo electrónico en miniatura que puede escuchar, transmitir y/o grabar una conversación. Al colocar un micrófono oculto en su hogar u oficina, las fuerzas del orden pueden escuchar todo lo que se dice dentro del rango de alcance del dispositivo. Los requisitos que rigen el uso de micrófonos ocultos suelen ser los mismos que los de las escuchas telefónicas. El uso de micrófonos ocultos conlleva algunas dificultades para los agentes de las fuerzas del orden: deben instalarse dentro del lugar objetivo, tienden a funcionar mal, existe el riesgo de que sean descubiertos y puede que se tornen inútiles por interferencia eléctrica. Debido a estas dificultades, existe una tendencia a usar menos micrófonos ocultos que escuchas telefónicas.

Registros de llamadas salientes y dispositivos de control y rastreo

Un registro de llamadas salientes graba los números que se marcan desde una línea telefónica a la cual está conectado el dispositivo. Los dispositivos de control y rastreo graban los números de teléfono de las llamadas entrantes.

Se necesita una orden judicial si las fuerzas del orden desean instalar y usar cualquiera de los dos dispositivos; sin embargo, estas órdenes judiciales son muy fáciles de obtener. El gobierno sólo necesita creer que la información que probablemente se obtenga es relevante para una investigación criminal en marcha. Los jueces y las fuerzas del orden típicamente adoptan una visión

Conozca las herramientas de ellos

Registros de llamadas salientes y dispositivos de control y rastreo (cont.)

muy amplia de lo que es probablemente relevante para una investigación. Muchos estados permiten ese tipo de vigilancia bajo estándares aún más flexibles. Además, el Fiscal General de los EE.UU. puede, en ciertas situaciones "de emergencia", autorizar el uso de estos dispositivos durante hasta siete días sin la obtención de una orden del juez.

La Ley patriota (Patriot Act) amplió el uso permitido tanto de registros de llamadas salientes como de dispositivos de control y rastreo. Entre algunos de los usos ampliados de los registros de llamadas salientes y dispositivos de control y rastreo se incluyen: rastreo de la ubicación física de usuarios de teléfonos celulares, registro de las direcciones de los sitios web que visita, las direcciones de protocolo de Internet (IP) a las que su computadora se conecta, o las direcciones IP que se conectan a su computadora. Una dirección IP es un número único asignado a cada computadora o dispositivo que se conecta a una red.

Conozca las herramientas de ellos

¿Qué hay del Tribunal de vigilancia de inteligencia extranjera y del Programa de escuchas telefónicas sin garantía de la Agencia de seguridad nacional?

El gobierno puede escuchar tanto a ciudadanos como a no ciudadanos si existe causa probable para creer que el blanco es miembro de un grupo terrorista extranjero o un agente de una potencia extranjera. A fin de escuchar a ciudadanos y a residentes legales permanentes, el gobierno debe además demostrar causa probable de que el blanco está involucrado en actividades que "tal vez" se relacionen con una violación delictiva.

Para este tipo de vigilancia, el gobierno debe obtener una orden de allanamiento del Tribunal de vigilancia de inteligencia extranjera, un tribunal secreto donde las audiencias y los registros no están abiertos al público. El gobierno, a través de la Agencia de seguridad nacional (NSA, por sus siglas en inglés), reclama la autoridad de controlar, sin ningún tipo de orden judicial, toda comunicación telefónica o electrónica si considerase que una parte está ubicada fuera de los EE.UU., e incluso si la otra parte estuviera dentro de los EE.UU. Si bien la NSA sólo está autorizada a controlar las comunicaciones con el fin de obtener datos de inteligencia extranjera, se desconoce el alcance total de este programa.

¿Qué amenazas de seguridad representan los teléfonos celulares, los teléfonos inteligentes y las PDA?

La practicidad y facilidad de la comunicación por teléfono celular trae consigo importantes riesgos de privacidad y seguridad. Tenga en cuenta los riesgos inherentes al uso de estos dispositivos y compare el beneficio de la practicidad con el riesgo de seguridad antes de usar el teléfono celular.

Las mismas reglas legales que se aplican a las líneas fijas se aplican a la obtención de un permiso de escucha, un registro de llamadas salientes o un dispositivo de control y rastreo para un teléfono celular. No obstante, es importante tener en cuenta que todos quienes dispongan de un equipo de unos pocos cientos de dólares de costo pueden interceptar las señales de su teléfono celular. Y no debe asumir que los agentes siempre respetan la ley. Las personas y las empresas también pueden interceptar con facilidad las señales de su teléfono celular corriendo poco riesgo de ser descubiertos.

El gobierno tiene la capacidad de convertir un teléfono celular en un dispositivo de escucha o en un "micrófono oculto ambulante". Esto permite al gobierno escuchar toda conversación que tenga lugar cerca del teléfono celular. El gobierno no necesita acceder al teléfono mismo para "plantar" un micrófono oculto, sino que simplemente puede hacerlo a través de su empresa proveedora de servicio telefónico celular.

Los micrófonos ocultos ambulantes permiten al gobierno escuchar conversaciones que tengan lugar cerca de su teléfono celular, incluso cuando el teléfono está apagado. Parece ser, no obstante, que quitarle la batería al teléfono celular desactivaría el micrófono oculto ambulante.

También se puede usar su teléfono celular para rastrear su ubicación. Siempre que su teléfono esté encendido y tenga señal, estará en contacto con una o más torres de telefonía celular de su área. El gobierno puede controlar estas conexiones para determinar su ubicación física. En ciudades y otras áreas con mayor densidad de torres de telefonía celular, su ubicación se puede rastrear con más exactitud, a veces dentro de un perímetro de pocas yardas. Actualmente no existe un estándar legal uniforme para este tipo de rastreo de teléfono celular. Algunos tribunales exigen a los agentes cumplir con escasa evidencia a fin de obtener un permiso para registro de llamadas salientes o dispositivo de control y rastreo, mientras que otros tribunales

¿Qué amenazas de seguridad representan los teléfonos celulares, los teléfonos inteligentes y las PDA? (continuación)

exigen a los agentes la obtención de una orden judicial respaldada por causa probable. El gobierno puede además repasar los registros antiguos de su teléfono celular para determinar su ubicación en un momento dado, si su teléfono estaba encendido.

Algunos tribunales han manifestado que, una vez que lo arrestan, las fuerzas del orden pueden, con orden judicial mediante, revisar el historial de llamadas y los contactos guardados en su teléfono celular. Algunos tribunales han llegado a manifestar que, luego de un arresto legal, las fuerzas del orden pueden examinar los mensajes de texto, fotos, correos electrónicos y demás registros que contenga su teléfono.

Algunos tribunales permiten a las fuerzas del orden revisar los historiales de llamadas sin una orden, argumentando que el historial de llamadas proporcionará la misma información que puede obtenerse con un registro de llamadas salientes, pero exigen una orden judicial para revisar mensajes de texto o correos electrónicos. Los tribunales aún están desarrollando este aspecto de la ley; como resultado de ello, las leyes y reglamentos varían de una jurisdicción a otra. La habilitación de protección con contraseña de su teléfono celular ofrece cierto nivel de protección contra los riesgos de seguridad inherentes al uso de teléfonos celulares.

¿Puede el gobierno controlar mis mensajes de texto?

Los mensajes de texto son un método considerablemente inseguro de comunicación. Al igual que las conversaciones por teléfono celular, los mensajes de texto pueden ser interceptados fácilmente por cualquier persona que tenga el equipo adecuado. Ni el Congreso ni los tribunales han sido claros con respecto a la necesidad de causa probable y de orden judicial para interceptar mensajes de texto, por lo que las fuerzas del orden podrían intentar interceptar mensajes de texto usando órdenes de registro de llamadas salientes o de dispositivos de control y rastreo, que son relativamente fáciles de obtener.

Finalmente, como los mensajes de textos no son considerados “comunicaciones por cable”, no están protegidos por la norma de

exclusión de la Ley de escuchas telefónicas. Por lo tanto, si el gobierno intercepta ilegalmente sus mensajes de texto, igualmente podrá usar estas comunicaciones contra usted en un juicio penal.

Comunicaciones por Internet

¿Puede el gobierno leer mi correo electrónico?

Las fuerzas del orden pueden acceder fácilmente a gran parte de sus comunicaciones electrónicas y a la información que contienen. Para obtener una orden judicial a fin de acceder a sus comunicaciones electrónicas, el gobierno sólo necesita demostrar que la información que es probable que se obtenga es relevante para una investigación penal en curso. Con la orden judicial, el gobierno puede obtener su "información básica de suscriptor", que incluye el nombre y la dirección física asociados con una cuenta, la extensión y los tipos de servicio utilizados, los inicios de sesión y la dirección IP de su computadora.

El gobierno necesita una Orden D (véase "Conozca las herramientas de ellos: Órdenes D") para obtener otros "registros sin contenido", que incluyen todo registro o bitácora que refleje las direcciones de correo electrónico que envía o de las que recibe correo, horas y fechas en los que envió o recibió correos electrónicos, y el tamaño de cada correo electrónico.

En cuanto a los correos electrónicos almacenados por terceros, como por ejemplo un servicio de correo electrónico en la web o un proveedor de servicios de Internet (ISP, por sus siglas en inglés), se aplican diferentes protecciones dependiendo de lo reciente que sea un correo electrónico y si lo ha leído usted o no.

La Ley de comunicaciones almacenadas (Stored Communications Act) exige a las fuerzas del orden la obtención de una orden de allanamiento para el contenido (línea de asunto y cuerpo) de los correos electrónicos no abiertos que se han almacenado por más de 180 días. En el caso de correos electrónicos no abiertos de más de 180 días de antigüedad, almacenados por un tercero, el gobierno puede obtener una Orden D o emitir una orden judicial para obtener el contenido de los correos electrónicos. El gobierno puede además optar por conseguir una

¿Puede el gobierno leer mi correo electrónico? (continuación)

orden de allanamiento en el caso de correos electrónicos de más de 180 días de antigüedad o de correos electrónicos abiertos.

En Alaska, Arizona, California, Hawai, Idaho, Montana, Nevada, Oregon y Washington, que son estados cubiertos por el Tribunal de apelaciones del Noveno Circuito, los tribunales no estuvieron de acuerdo con la interpretación del gobierno con respecto a que puede, con una Orden D, obtener correos electrónicos abiertos que se han almacenado por más de 180 días. Estos tribunales han determinado que el gobierno necesita una orden judicial para cualquier correo electrónico que tenga menos de 180 días de antigüedad.

Se supone que el gobierno debe dar previo aviso al abonado individual cuando vaya a usar Órdenes D u órdenes judiciales para obtener el contenido del correo electrónico. En teoría, esto permitiría al abonado proceder a anular la orden judicial antes de que el tercero cumpla con ella.

Otra disposición de la Ley de comunicaciones almacenadas, no obstante, permite a las fuerzas del orden retrasar la notificación de una orden D u orden judicial durante un período de tiempo considerable, y parece ser que el gobierno retrasa la notificación a menudo.

Las fuerzas del orden también pueden evitar notificarlo, tomando las medidas adicionales requeridas para una orden de allanamiento.

Los ISP más grandes, según se informa, reciben más de 1000 órdenes judiciales por mes que procuran información sobre sus usuarios. La mayoría de las órdenes judiciales solicitan los nombres de usuario, las direcciones, las direcciones ISP y los registros de cuándo el blanco inició sesión y se desconectó de Internet.

Hay muchos informes de programas de las fuerzas del orden diseñados para captar grandes cantidades de tráfico por Internet, incluyendo correos electrónicos y actividad en la web.

El alcance de estos programas, su uso permitido y la admisibilidad de toda información obtenida a través de ellos en un tribunal se desconoce actualmente.

¿Puede el gobierno saber qué sitios web visito?

Las fuerzas del orden necesitan una orden judicial para la obtención de los registros de sitios web que usted visita. El gobierno puede, según se informa, obtener direcciones de localizador uniforme de recursos (Uniform Resource Locator, URL por sus siglas en inglés), p. ej. http://ccrjustice.org, de sitios web que usted haya visualizado, sin una orden judicial, pero necesita una orden para obtener información sobre páginas específicas que usted haya visitado en un sitio web, p. ej. http://ccrjustice.org/ifanagentknocks.

¿Debo tener cuidado con la vigilancia electrónica por parte de una entidad no gubernamental?

El espionaje corporativo es una industria probablemente mayor que el espionaje gubernamental. Las empresas suelen contratar espías particulares, la mayoría de los cuales son ex agentes de las fuerzas del orden, para vigilar a activistas que pudieran amenazar sus intereses. El espionaje corporativo comprende muchas de las mismas tácticas empleadas por el gobierno, incluyendo: revisar la basura, intervenir teléfonos, controlar la actividad en Internet y emplear infiltrados. Los espías corporativos probablemente se preocupen menos por las restricciones legales del espionaje.

"Órdenes D"

Otra herramienta de las fuerzas del orden es la Orden 2307(D), comúnmente denominada "Orden D". La Orden D obtiene su nombre de la subsección de la Ley de comunicaciones almacenadas que las autoriza. El gobierno usa órdenes D para obtener registros electrónicos almacenados por terceros, por lo general correo electrónico. Las órdenes D son más difíciles de obtener que una orden judicial simple, pero más fáciles de obtener que una orden de allanamiento. Para obtener una orden D, el gobierno debe proporcionar datos específicos a un juez que demuestren que existen fundamentos razonables para creer que la información que se busca es relevante para una investigación penal en curso. Por lo tanto, la sospecha necesaria para la orden D es menor que una causa probable, pero mayor que el estándar de "cualquier posibilidad razonable" necesario para obtener una orden judicial.

⚠ Conozca las herramientas de ellos

Cartas de seguridad nacional

La Carta de seguridad nacional (NSL, por sus siglas en inglés) es una herramienta usada por el FBI para solicitar secretamente información sobre una persona a un tercero, como por ejemplo una empresa telefónica, un ISP, una agencia de crédito al consumidor o una institución financiera. Las NSL no exigen causa probable ni supervisión; el FBI tan sólo necesita creer que la información que busca es relevante para una investigación de terrorismo o espionaje. La ley de NSL tiene una norma mordaza incorporada que prohíbe a quien reciba una NSL decir a alguien que no sea su abogado que la ha recibido. Si bien un fallo reciente en tribunal encontró que la norma mordaza incorporada y permanente es inconstitucional, no queda clara su futura aplicación.

Los estudios del gobierno han reportado que el FBI emite decenas de miles de NSL por año, y que a menudo viola incluso las menores restricciones de su autoridad para emitirlas. Los datos de las NSL se comparten dentro de la comunidad de inteligencia de los EE.UU., con otras agencias gubernamentales e incluso con gobiernos extranjeros.

Si usted o la organización donde trabaja reciben una NSL, pónganse en contacto con un abogado inmediatamente.

Conozca las herramientas de ellos

Seguridad electrónica

La seguridad electrónica es un tema inmenso y complejo. Esta sección presenta algunos consejos básicos acerca de la seguridad electrónica. Encontrará información más detallada sobre cada uno de estos temas en la sección Recursos adicionales de este folleto.

Dicho simplemente, la comunicación electrónica más segura es no entablar ninguna comunicación electrónica. Los hábitos de seguridad electrónica eficaces requieren que se mantenga un equilibrio constante entre la practicidad y los riesgos asociados con la comunicación electrónica. Al igual que con cualquier práctica, debe sopesar riesgos y beneficios al decidir qué medidas de seguridad electrónica emplear.

Cifrado de datos

El cifrado es un método de codificar la información. Si se usa correctamente, el cifrado protege su información para que no la vea nadie que no tenga la "clave" adecuada para verla. La tecnología moderna de cifrado es lo suficientemente fuerte como para que sea prácticamente imposible para el gobierno descifrar mensajes cifrados sin el uso de claves. El cifrado es la protección más potente con la que cuenta para evitar que el gobierno obtenga su información electrónica.

Hay programas ampliamente disponibles que le permiten cifrar toda la información de su disco duro. Las simples contraseñas de inicio de sesión en su computadora no son suficientes para proteger su disco duro.

El gobierno puede tomar el disco duro, hacerle una copia y acceder fácilmente a los datos sin su contraseña de inicio de sesión. Con un disco duro cifrado, sus archivos estarán codificados y el gobierno no podrá acceder a ellos sin su contraseña de cifrado.

Los programas de cifrado también permiten cifrar archivos o carpetas individuales. Si bien tal vez esto sea más sencillo de manejar, el cifrado realizado poco a poco podría dejar esos archivos más vulnerables. Una mejor solución es mantener un disco duro aparte, totalmente cifrado, con los archivos delicados.

Conozca las herramientas de usted

Seguridad electrónica

Cifrado de correos electrónicos

El uso de cifrado es aún más importante en el caso del correo electrónico. Ya hemos mostrado cómo el gobierno puede usar órdenes D u órdenes judiciales para acceder fácilmente a su correo electrónico, o usar otras herramientas para interceptarlo durante su transmisión. Y, una vez que un correo electrónico está en la computadora de un tercero, usted ya no tiene control sobre quién lo recibirá y leerá. De manera similar al cifrado de datos, una herramienta para proteger sus comunicaciones electrónicas es el cifrado de correo electrónico. A fin de utilizar efectivamente el cifrado de correo electrónico, no obstante, tanto usted como quien sea con quien se está comunicando deben usar un programa de cifrado.

El cifrado de correo electrónico garantiza que sólo los destinatarios deseados puedan leer el correo electrónico que usted envía. El cifrado moderno de correo electrónico funciona mediante un sistema de "claves públicas". Una clave pública proporciona instrucciones, o el código, para saber cómo se deben codificar los correos electrónicos que le envíen. El código para decodificar mensajes (la "clave privada") es distinto a la clave pública, y sólo usted tiene acceso a la clave privada. Si sus correos electrónicos son interceptados a través de una orden judicial u otro documento, los mensajes allí contenidos no se pueden decodificar sin su clave privada.

Si bien los aspectos más técnicos del cifrado de correo electrónico son demasiado detallados como para ser incluidos en este folleto, una analogía simple del cifrado es una puerta abierta que cualquiera puede trancar pero que sólo quien tenga una llave especial podrá abrir.

El cifrado de correo electrónico es más fácil de usar hoy de lo que era en el pasado. El GNU Privacy Guard (GnuPG) es un programa gratuito que se puede integrar a la mayoría de los principales programas de correo electrónico. Por ejemplo, el cliente de correo electrónico de terceros Mozilla Thunderbird ofrece un plug-in (complemento), también conocido como extensión de seguridad, llamado Enigmail, que es compatible con GniPG y hace que el cifrado sea bastante fácil de usar.

Conozca las herramientas de usted

Seguridad electrónica

Contraseñas

Tómese en serio las contraseñas. No use una palabra ni una palabra con un número al final o en el medio. Esas contraseñas se pueden quebrar fácilmente luego de unos pocos intentos. Use una serie de caracteres que sólo tengan sentido para usted.

No use dos veces la misma contraseña para ninguna cuenta que tenga información privada. Intente guardar sus contraseñas en la mente. Las contraseñas escritas pueden ser descubiertas, u obtenidas por orden judicial. Cambie las contraseñas cada dos o tres meses. Si anota sus contraseñas, intente hacerlo en un código que sólo usted entienda. Si decide anotar una contraseña, jamás la deje junto a la computadora o cerca de la misma; es mejor que la guarde en la cartera.

Tenga en cuenta usar un programa de "contraseñas aseguradas". Estos programas le permiten guardar sus contraseñase en un único archivo cifrado en su computadora, por lo que sólo deberá memorizar una contraseña para acceder a todas sus demás contraseñas. No anote su contraseña principal, ya que esta es la contraseña que protege a todas las demás.

Navegación por Internet

Administre con cuidado los datos que su explorador web pueda guardar de su actividad de Internet y los datos que otros sitios web puedan tener sobre usted.

Por defecto, los navegadores de Internet guardan gran cantidad de información potencialmente privada, incluyendo entre otras cosas: los sitios web que visita, las contraseñas de esos sitios web e incluso imágenes de las páginas web que visita. Un agente que eche mano a su disco duro puede aprender mucho acerca de su actividad en Internet a partir de estos archivos. Borre esta información periódicamente. Configure su navegador para que periódicamente borre su historial de navegación en Internet, caché, cookies, historial de descargas, formularios guardados y contraseñas guardadas. Tal vez desee hacerlo a diario, o cada vez que cierre el navegador.

Siempre que esté disponible, use el cifrado incorporado de un sitio web al navegar, para evitar que terceros intercepten la información transmitida. Los sitios web que tienen cifrado incorporado empiezan con https:// en vez de http://. Tenga en cuenta usar herramientas anónimas de Internet, como por ejemplo

Conozca las herramientas de usted

Seguridad electrónica

Navegación por Internet (cont.)

Tor.

Tor es un programa de cifrado y anonimato que enruta sus datos sólo a través de otros clientes de Tor, cifrando sus datos en el proceso y eliminando la información acerca del origen de los datos. Cada enrutador Tor conoce sólo la dirección del último enrutador que atravesó, lo cual hace que sea sumamente difícil rastrear cualquier comunicación hasta su punto de origen. Algunos inconvenientes del uso de Tor son velocidades más lentas de carga de páginas web, y que muchas funciones inseguras, como Flash, no funcionan a través de Tor.

Conozca a sus proveedores de servicio de Internet

Lea las condiciones de servicio y las políticas de privacidad de todo servicio electrónico que esté pensando en contratar. Algunos ISP, incluyendo varios que están hechos a la medida de las necesidades de los activistas políticos, ofrecen mayores protecciones de la privacidad y dicen ser más resistentes al espionaje del gobierno.

Uso de programas antispyware

Compre un buen programa antispyware y antivirus y actualícelo periódicamente. El spyware puede violar toda su seguridad electrónica, y sabrá acerca de cada sitio web que visite y cada tecla que pulsa en su máquina. Las principales empresas antispyware dicen que tratan el spyware del gobierno de la misma forma que los demás spyware.

Retención y eliminación de datos

El gobierno no puede obtener lo que no existe. Establezca una política de retención de datos donde revise y elimine archivos viejos sistemáticamente. No destruya documentos de manera selectiva; escoja un momento determinado y respételo. Puede disponer un momento distinto para distintos tipos de datos, p. ej. borrar archivos de computadora cada dos meses, borrar correos electrónicos cada dos semanas y borrar historiales del navegador web cada dos días. Sea cual sea la política, respétela. Después de todo, ¿realmente necesita los correos electrónicos

Conozca las herramientas de usted

Seguridad electrónica

Retención y eliminación de datos (continuación)

de los últimos tres años?

No destruya nada que le haya sido requerido por orden judicial: si lo hace, corre riesgo de ser acusado de obstrucción de la justicia. Lleve un registro escrito de su política de retención de datos para protegerse y proteger a su organización contra acusaciones de destrucción de evidencia.

Conozca las herramientas de usted

Grandes Jurados y resistencia al Gran Jurado

¿Qué son los Grandes Jurados y qué amenazas representan para los activistas?

Un gran jurado es un panel de ciudadanos que se reúne para investigar delitos y emitir fallos. En su concepción original, se suponía que los grandes jurados eran radicalmente democráticos. En Inglaterra, servían como amortiguador entre los ciudadanos y el monarca y sus abogados. En los primeros tiempos de Estados Unidos, cualquier ciudadano podía presentar una acusación de mal obrar ante el gran jurado original, y dicho gran jurado podía fallar por voto de la mayoría.

Los grandes jurados de hoy en día son muy distintos. Hoy por hoy, es el fiscal quien presenta todos los casos ante un gran jurado. El fiscal elige a los testigos y hace las preguntas. Los testigos no pueden tener un abogado presente. No hay un juez presente. El fiscal redacta los cargos y se los lee al gran jurado. No es obligatorio que los miembros del gran jurado tengan conocimiento de la ley en cuestión. Y, a diferencia de otros jurados, los miembros del gran jurado no son sometidos a evaluaciones de imparcialidad.

En el caso extraordinario de que un gran jurado no falle, el fiscal simplemente puede constituir otro gran jurado y procurar un fallo ante un nuevo gran jurado.

Como el fiscal sólo orquesta las demandas, no es sorpresa que los grandes jurados casi siempre sirvan de aval de la parte acusadora. Es famoso un antiguo juez principal de Nueva York que una vez observó que “cualquier fiscal que lo desee podría acusar a un sándwich de jamón”.

¿Qué son los Grandes Jurados y qué amenazas representan para los activistas? (continuación)

En casos políticos, se han usado grandes jurados para llevar a cabo cacerías de brujas contra activistas. Los fiscales presentarán testigos activistas e intentarán que estos delaten a otros activistas bajo amenaza de encarcelación si se niegan a cooperar con el gran jurado.

Es fundamental entender cómo funciona un gran jurado, cuáles son sus derechos, qué derechos no puede ejercer y cómo resistirse a un gran jurado.

Muchos derechos que damos por sentados no existen para testigos ante un gran jurado. Los testigos ante un gran jurado no tienen derecho a ser representados por un abogado ni tienen derecho a un juicio con jurado si los amenazan con ir a la cárcel. Los testigos ante grandes jurados conservan el derecho contra la autoincriminación, pero a pesar de ello pueden forzarlos a delatarse a ellos mismos y a terceros a cambio de inmunidad ante acusaciones y castigos. La inmunidad sólo protege a los testigos; los terceros igualmente podrán ser acusados.

¿Qué debo hacer si alguien se presenta con una orden de comparecencia de un Gran Jurado?

Las órdenes de comparecencia del gran jurado son presentadas por agentes de las fuerzas del orden, generalmente oficiales de policía o alguaciles federales. Una orden de comparecencia de un gran jurado debe serle entregada personalmente, es decir, en mano. Si se niega a aceptarla, deben dejarla cerca suyo.

Una orden de comparecencia de un gran jurado no otorga a un agente el derecho de revisar un hogar, una oficina, un auto ni ningún otro lugar, ni lo obliga a usted a entregar ningún documento ni a decir nada en ese momento. Una orden de comparecencia ante un gran jurado sólo le exige que haga algo en la fecha futura especificada en la orden.

Si un agente se presenta ante usted e intenta entregarle una orden de comparecencia, acéptela y no haga nada más. No responda ninguna pregunta, no autorice revisiones y no lo invite a pasar a su casa por ningún motivo.

Órdenes de comparecencia del gran jurado

Los grandes jurados obtienen información de las personas emitiendo órdenes de comparecencia. Una orden de comparecencia de un gran jurado es una orden para testificar ante un gran jurado o de proporcionar determinada información al gran jurado. Los grandes jurados emiten distintos tipos de órdenes de comparecencia para testimonios e información. Una orden ad testificandum, o para testificar, es una orden que obliga al testigo a comparecer y dar testimonio. Una orden duces tecum, que quiere decir "tráigalo consigo" en latín, es una orden que obliga al testigo a proporcionar al gran jurado determinados documentos. Los grandes jurados también usan estas órdenes para obtener huellas dactilares y muestras de caligrafía. Los grandes jurados suelen emitir ambas órdenes para el mismo testigo, para así poder obtener tanto los documentos como el testimonio.

⚠ Conozca las herramientas de ellos

¿Qué opciones tengo si recibo una orden de comparecencia de un Gran Jurado?

Una vez que haya recibido una orden de comparecencia del gran jurado, normalmente tiene tres opciones: 1) puede cumplir con la orden de comparecencia, 2) puede proceder a anular la orden de comparecencia, o 3) puede rehusarse a obedecer. Si recibe una orden de comparecencia, debe ponerse en contacto con un abogado lo antes posible y hablar detalladamente de cada una de estas opciones.

Cumplir con una orden de comparecencia es relativamente sencillo. En el caso de una orden ad testificandum, debe presentarse en la fecha, hora y lugar estipulados en la orden y responder las preguntas del fiscal. En el caso de una orden duces tecum, debe presentarse en la fecha, hora y lugar estipulados en la orden con los documentos o demás evidencia solicitada.

Si cumple con una orden de comparecencia, evita la posibilidad de ser castigado por ignorarla; no obstante, cumplir con dicha orden tal vez le traiga otro tipo de problemas. Por ejemplo, si es usted el blanco de la investigación, cumplir con la orden tal vez proporcione al gobierno información que necesita a fin de acusarlo y condenarlo. Tal vez ponga además en riesgo a otro activista al cumplir con la orden de comparecencia.

Si recibe una orden de comparecencia, debe hablar con un abogado antes de hacer nada. Si la orden de comparecencia tiene motivación política, lo ideal es que hable con un abogado de su círculo de activismo que se ocupe de defensa penal o de casos ante el

¿Qué opciones tengo si recibo una orden de comparecencia de un Gran Jurado? (continuación)

gran jurado.

Es posible que algunos abogados penales defensores no activistas le sugieran convertirse en delator. No obstante, es importante tener en cuenta que muchos delatores terminan condenados a tantos años de cárcel como las personas a quienes delatan.

Los procesos del gran jurado son secretos. La comunidad activista a menudo ignora cuándo se está desarrollando una investigación del gran jurado. Como resultado, muchos activistas creen que deberían hacer público el hecho de haber recibido una orden de comparecencia. Esta podría ser una táctica efectiva a explorar con su abogado en caso de recibir una orden de comparecencia.

¿Cómo anulo una orden de comparecencia de un Gran Jurado?

Puede desafiar una orden de comparecencia ante un tribunal presentando una moción de anulación de la orden de comparecencia. La anulación de una orden de comparecencia significa que un tribunal la declare nula. Un tribunal aprobará una moción de anulación sólo si hubiera fundamentos jurídicos suficientes, como por ejemplo error de identificación, ausencia de jurisdicción, un privilegio protegido o una base ilegal de los procedimientos.

Aunque no pueda anular una orden de comparecencia con éxito, el litigio de una moción de anulación ante un tribunal podría conseguirle un poco de tiempo. El tiempo es importante, en especial si no tiene pensado cooperar con el gran jurado, porque si no coopera podría ir a la cárcel. Los grandes jurados pueden durar hasta 18 meses; cualquiera sea el tiempo que dure el litigio de la moción de anulación, podría ahorrarle la experiencia de pasar todo ese tiempo en la cárcel.

Si bien hay poco que perder al presentar una moción de anulación de una orden duces tecum, las órdenes judiciales que exigen pruebas, las mociones de anulación de órdenes ad testificandum, que exigen testimonio, podrían presentar problemas. Al menos un tribunal de distrito federal ha emitido el fallo de que uno pierde toda objeción que no se haya mencionado en la moción de anulación original. No debe renunciar a sus objeciones, en especial porque tal vez no sepa

cuáles son sus objeciones hasta que le hagan una pregunta en particular.

Un buen abogado político debe ser capaz de aconsejar si es buena idea proceder con una anulación de orden de comparecencia, o si no es conveniente dadas sus circunstancias particulares.

¿Qué pasa si me niego a cumplir con una orden de comparecencia de un Gran Jurado?

Hay dos formas básicas de rehusarse a cumplir con una orden de comparecencia de un gran jurado: 1) rehusarse a comparecer y 2) rehusarse a responder las preguntas del fiscal.

Si simplemente se rehúsa a comparecer para dar su testimonio, tal vez lo declaren en desacato y el gobierno podrá optar por arrestarlo y encarcelarlo hasta que testifique o hasta que el gran jurado caduque. Si su testimonio no es particularmente importante para el fiscal, tal vez opten por no tomar ninguna medida.

¿Qué pasa si cumplo con una orden de comparecencia de un Gran Jurado?

Si comparece a testificar, no le permitirán tener a su abogado presente. No obstante, puede tener a su abogado en la puerta de la sala del gran jurado, y puede consultar con él después de cada pregunta, aunque algunos tribunales han determinado que sólo puede consultar a su abogado después de una serie de preguntas.

Como usted conserva su derecho de la Quinta Enmienda contra la autoincriminación, puede negarse a responder las preguntas del fiscal diciendo “Invoco mi privilegio de la Quinta Enmienda contra la autoincriminación” después de cada pregunta.

A este punto, el fiscal sencillamente lo dejará ir, o tal vez busque otorgarle inmunidad.

La inmunidad impide que el testigo reciba acusaciones penales sobre la base del testimonio ante el gran jurado. El otorgamiento de inmunidad debe contar con la aprobación de un juez.
Un fiscal puede lograr que un juez apruebe previamente un otorgamiento de inmunidad; otra posibilidad es que el testigo sea llevado ante un juez quien, según el fiscal lo solicite, casi siempre otorga la inmunidad.

¿Qué pasa si cumplo con una orden de comparecencia de un Gran Jurado? (continuación)

Si usted sigue negándose a responder las preguntas luego de haber obtenido inmunidad, el fiscal puede llevarlo ante un juez, quien le ordenará que testifique. Si sigue rehusándose, el juez puede enviarlo a la cárcel por desacato civil. Los testigos que se rehúsan a proporcionar muestras materiales, p. ej. muestras de caligrafía, cabello, presencia en una alineación de sospechosos o documentos, según lo solicite un gran jurado, también podrán ser encarcelados por desacato civil.

Si bien el desacato civil no es un delito, puede provocar la encarcelación del testigo mientras dure el gran jurado. Los grandes jurados pueden durar hasta 18 meses, aunque algunos grandes jurados "especiales" pueden obtener hasta tres extensiones de seis meses cada una. El propósito de la encarcelación de un testigo obstinado es coaccionarlo para que testifique.

A veces los jueces liberan a testigos antes de la disolución del jurado si queda claro que no existe posibilidad alguna de que el testigo testifique.

El gobierno también puede acusar de "desacato penal" a testigos que no cooperen con el gran jurado.

El gobierno también puede acusar de "desacato penal" a testigos que no cooperen con el gran jurado.
El desacato penal no conlleva una sanción máxima: la sentencia depende totalmente del criterio del juez. Si bien el desacato civil pretende coaccionar a un testigo para que testifique, el desacato penal pretende castigar a un testigo por obstaculizar el proceso legal. Como con cualquier otro delito, el desacato penal requiere una notificación de cargos, el derecho a recibir asistencia legal y prueba más allá de la duda razonable. Los cargos de desacato penal son sumamente excepcionales.

Si lo encarcelan, podrá presentar periódicamente una moción manifestando que: 1) la cárcel no lo coaccionará para testificar y 2) su reclusión es simplemente punitiva, y por lo tanto, inconstitucional. Si gana una de estas mociones, será liberado.

Algunos activistas crean expedientes para estar preparados en caso de ser convocados ante un gran jurado. Un expediente que haga constar por escrito su convicción incondicional de no cooperar con procedimientos del gran jurado se puede usar como evidencia de que en su

caso no funcionará declararlo en desacato civil, y por lo tanto lo ayudará a ser liberado.

¿Qué pasa después de un Gran Jurado?

Lo que sucede en un proceso del gran jurado es secreto. El gobierno confía en este secreto para generar temor y desconfianza en comunidades activistas. Algunos activistas han disipado ese temor y esa desconfianza exitosamente entre comunidades activistas, publicando las preguntas que les formuló el fiscal y las respuestas proporcionadas. Si tiene pensado actuar de esta manera, debe hablar con un abogado para asegurarse de no estar creando más problemas de los que está resolviendo.

Consideraciones especiales para no ciudadanos

Los no ciudadanos son personas que no tienen la ciudadanía estadounidense, incluyendo turistas, estudiantes y demás personas que estén en los EE.UU. con visas o programas que exoneran del requisito de visa, residentes legales permanentes, refugiados y aquellos sin estado de inmigración legal. Los no ciudadanos en los EE.UU. comparten la mayoría de los derechos constitucionales de los ciudadanos. Existen algunas excepciones a la regla, y los no ciudadanos que se involucren en activismo político deben tener en cuenta varias consideraciones especiales. No obstante, los no ciudadanos no deben evitar por completo el activismo político sobre la base de un temor irracional de represión por parte del gobierno.

Discursos y filiaciones políticas

En la mayoría de los casos, el gobierno trata al discurso de los no ciudadanos de la misma manera que trata el discurso de los ciudadanos. Los no ciudadanos no pueden ser castigados penalmente por discursos que estarían protegidos si los manifestara un ciudadano. De manera similar, los no ciudadanos no pueden ser demandados por un discurso que estaría protegido si lo hubiera dicho un ciudadano.

No obstante, el gobierno tiene amplios poderes para retener los beneficios de inmigración (tales como el remedio discrecional o la naturalización), y potencialmente podrá incluso iniciar procedimientos de deportación basándose en el discurso de un no ciudadano.

No queda claro si el gobierno puede expulsar a un no ciudadano o solamente retener sus beneficios discrecionales de discurso o asociación política.

Cincuenta años atrás, algunos tribunales determinaron que el

Discursos y filiaciones políticas (continuación)

gobierno podía hacerlo, pero la ley de la Primera Enmienda ha cambiado drásticamente desde entonces, y ahora los tribunales están divididos con respecto a si esa norma sigue siendo una ley válida. Hablando desde el punto de vista práctico, es sumamente excepcional que el gobierno deporte a alguien basándose únicamente en un discurso o asociación.
Sin embargo, el gobierno está autorizado a hacer regir selectivamente las leyes de inmigración.

Por ejemplo, el gobierno puede deportar a no ciudadanos por violaciones de la ley de inmigración (como por ejemplo quedarse más tiempo del permitido por la visa, o por trabajar sin autorización), incluso si la motivación del gobierno para iniciar los procedimientos de deportación es un discurso o una asociación política de no ciudadanos.

Finalmente, los solicitantes de residencia permanente y naturalización deben enumerar las organizaciones para las que han trabajado. Se recomienda a los no ciudadanos políticamente activos que consulten con un abogado de inmigración antes de solicitar un cambio de estado, porque algunas asociaciones podrían causarle problemas en su proceso de solicitud.

Búsquedas y confiscaciones

Los no ciudadanos gozan plenamente de la misma protección de la Cuarta Enmienda contra búsquedas y confiscaciones poco razonables que gozan los ciudadanos. Las fuerzas del orden deben obtener una orden de allanamiento para realizar cualquier búsqueda a un no ciudadano o en la propiedad de un no ciudadano, tal como deben hacer para realizar una búsqueda a un ciudadano. La evidencia que se obtenga mediante violación de la Cuarta Enmienda queda excluida del juicio penal de un no ciudadano, tal como sucedería con los ciudadanos.

Lamentablemente, el uso de evidencia obtenida violando la Cuarta Enmienda suele ser admitida en procesos de inmigración. Esto quiere decir que el gobierno puede usar evidencia obtenida de manera ilegal, que no puede usarse en procesos penales, para procesos de inmigración. Es posible que la evidencia obtenida a través de violaciones particularmente atroces de la Cuarta Enmienda sea excluida en procesos de inmigración.

Además, generalmente el gobierno puede revisar y confiscar a toda persona, paquete o vehículo

Búsquedas y confiscaciones (continuación)

que atraviese la frontera o en un aeropuerto.

Derecho a guardar silencio

Los no ciudadanos generalmente tienen el mismo derecho a guardar silencio que los ciudadanos. Si los agentes de las fuerzas del orden lo interrogan, puede guardar silencio y rehusarse a responder sus preguntas, aunque lo detengan o arresten temporalmente. Simplemente puede no decir nada, o decir algo como “Me gustaría hablar con mi abogado antes de decirle algo a usted” o “No tengo nada que decirle. Hablaré con mi abogado y él se comunicará con usted”. No firme nada sin leerlo y comprender plenamente las consecuencias de firmarlo.

Una excepción a esta regla es si un funcionario de inmigración pide a un no ciudadano que proporcione información relacionada con su estado de inmigración, incluso en esta situación, igual puede declarar que le gustaría que un abogado esté presente antes de que responda las preguntas.

La ley también exige a los no ciudadanos adultos que tengan documentos de inmigración válidos que los lleven consigo en todo momento. Si un agente le pide los documentos y se niega a dárselos, podrán acusarlo de un delito menor.

Nunca muestre papeles de inmigración falsos ni diga ser ciudadano de los EE.UU. si no lo es. En cambio, debe guardar silencio o decir que le gustaría hablar con un abogado. Mentir a un agente federal es un delito mucho más grave que el delito menor de no poder mostrar documentos; es mejor no mostrar nada que mostrar documentos falsos. Además, manifestar falsamente que es ciudadano podría impedirle obtener un estado legal o la ciudadanía en el futuro.

Conclusión

Tal como se mencionó anteriormente, la información presentada en este folleto es un manual de sus derechos básicos. Esta guía pretende ayudarlo a prepararse, a preparar a su organización y a sus compañeros activistas a estar plenamente informados y protegidos en caso de que un agente llame a su puerta. Y recuerde, los distintos estados tienen distintas leyes; es buena idea aprender las leyes de su estado y tener acceso a un abogado que las conozca bien.

Esperamos que este folleto pueda ser una herramienta para usted y su organización mientras trabajamos en pos de un mundo con más justicia social.

Para obtener copias de esta publicación, entre en http://ccrjustice.org/ifanagentknocks o escriba directamente a iaak@ccrjustice.org.

Recursos adicionales

Acerca de Prácticas generales de seguridad

Security Culture: a Handbook for Activists: una excelente revista de activistas canadienses que trata por qué construir una cultura de seguridad, y cómo hacerlo.
http://security.resist.ca/personal/culture.shtml

Security Survival Skills, por Collective Opposed to Police Brutality: una explicación de cómo construir una cultura de seguridad en su comunidad activista, realizada por un grupo en Canadá.
http://www.why-war.com/files/Securite-eng-letter.pdf

War at Home, por Brian Glick: un libro exhaustivo sobre la historia de COINTELPRO y excelentes consejos sobre cómo evitar los mismos problemas y protegerse a sí mismo y a su comunidad. Publicado por South End Press.

Acerca de los agentes del gobierno

The Attorney General's Guidelines on FBI Undercover Operations: las normas del gobierno federal sobre lo que pueden y no pueden hacer los agentes encubiertos.
http://www.usdoj.gov/olp/fbiundercover.pdf

The Attorney General's Guidelines Regarding the Use of Confidential Informants: las normas del gobierno federal sobre lo que pueden y no pueden hacer los informantes.
http://www.usdoj.gov/olp/dojguidelines.pdf

Security Practices and Security Culture: consejos básicos sobre cómo manejar las operaciones encubiertas y excelentes anécdotas de la época de COINTELPRO.
http://aia.mahost.org/sec_cointelpro.htm

Acerca de la seguridad telefónica

Mobile Surveillance Primer: un recurso en Internet muy completo sobre tecnologías de teléfonos celulares, cómo acceder a ellos y cómo proteger la información guardada en los teléfonos celulares y las conversaciones.
http://mobileactive.org/wiki/Mobile_Surveillance-A_Primer

Acerca de las Cartas de seguridad nacional

A Review of the FBI's Use of National Security Letters, por el Departamento de Justicia: una revisión profunda de la ley acerca de las Cartas de seguridad nacional y cómo se usan desde sus comienzos.
http://www.usdoj.gov/oig/special/s0703b/final.pdf

Acerca de la seguridad informática

Computer Security Trainer's Guide, por Midnight Special Law Collective: una guía realmente excelente para desarrollar buenos hábitos de seguridad con las computadoras en vez de instalar software o usar trucos técnicos.
http://www.midnightspecial.net/materials/trainers.html

NGO in a Box: Security Edition, por Tactical Technology Collective y Front Line Human Rights Defenders: un juego de herramientas para ayudar a los activistas y realizadores de medios independientes a establecer seguridad digital y a proteger su privacidad. El juego de herramientas incluye guías de herramientas de cifrado, herramientas de limpieza de virus, adware y spyware, almacenamiento de datos, protección de contraseñas, etc. Disponible gratis en Internet.
http://security.ngoinabox.org

Surveillance Self Defense, por Electronic Frontier Foundation: un excelente recurso en Internet sobre cómo protegerse de todo tipo de vigilancia electrónica. Para obtener datos específicos sobre seguridad de computadoras, consulte "Data Stored on Your Computer" (datos almacenados en su computadora) y "Defensive Technology" (tecnología defensiva).
https://ssd.eff.org

Acerca de vigilancia de alta tecnología

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, por la ACLU: un libro blanco sobre la historia reciente de las cámaras de vigilancia y otras tecnologías.
http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf

Acerca de los Grandes Jurados

Grand Jury Trainers Guide, por Midnight Special Law Collective: una explicación de los grandes jurados, desde el primer contacto con los agentes federales hasta la audiencia misma ante el gran jurado, y cómo protegerse y proteger a su comunidad si lo convocan a una.
http://www.midnightspecial.net/materials/trainers.html#gj

Agradecimientos y reconocimientos

Cuarto edición publicada en Abril de 2011

Center for Constitutional Rights
666 Broadway, 7th Floor
New York, NY 10012
www.CCRJustice.org / (212) 614-6464

El Centro para los derechos constitucionales (CCR, por sus siglas en inglés) se dedica a fomentar y proteger los derechos garantizados por la Constitución de los Estados Unidos y la Declaración Universal de Derechos Humanos. Fundado en 1966 por abogados que representaban a los movimientos de derechos civiles en el sur, el CCR es una organización jurídica y educativa sin fines de lucro comprometida con el uso creativo de la ley como una fuerza positiva para el cambio social. Visite www.ccrjustice.org.

Autor principal, Matthew Strugar, abogado integrante del personal del CCR. "Si un agente llama a su puerta" fue preparado por empleados y pasantes del CCR, entre los que se incluyen Lauren Melodia, Rachel Meeropol, Alison Roh Park, Qa'id Jacobs, Jeff Deutch, Arwa Fidahusein, Cathe Giffuni, Toni Holness, Carolyn Hsu, Jessica Juárez, Kenneth Kreuscher, David Mandel-Anthony y Christina Stephenson.

Traducción por Morningside Transaltions
El arte de portada fue realizado por Robert Trujillo (2011)
Fotografías de Maddy Miller (págs. 5, 9, 15)
Fotografías de SSGT Reynoldo Ramón, USAF (pág. 21)
Fotografías de Jarek Tuszynski (pág. 36)
Fuentes utilizadas: Georgia (cuerpo del texto), Distro (encabezados), Fluoxetine (encabezados)
Íconos realizados por pixel-mixer.com
Diagramación: Qa'id Jacobs

Descargo de responsabilidad: este folleto tiene únicamente fines informativos y no constituye asesoramiento legal. La intención del CCR es proporcionar una descripción general de los asuntos legales y prácticos que pueden enfrentar los activistas progresistas o radicales. Las circunstancias de cada persona son únicas, y diferencias fácticas menores podrían resultar en respuestas muy distintas a las preguntas que aquí se presentan. Para obtener respuesta a problemas, asuntos o preguntas legales específicas, obtenga el asesoramiento de un abogado calificado en su área.

Si un agente golpes

centerforconstitutionalrights

on the front lines for social justice