إذا جاء عميل يطرق الأبواب

centerforconstitutionalrights

on the front lines for social justice

جدول المحتويات

المقدمة

تتسم وكالات تطبيق القانون مثل المكتب الفدرالي للتحقيقات (FBI) بسجل مظلم من استهداف الحركات الراديكالية والتقدمية. ومن بين الحيل القذرة التي يستخدمونها ضد مثل هذه الحركات: اختراق صفوف تلك المنظمات لتشويه عملياتها وزعزعتها؛ وشن حملات من المعلومات المضللة والروايات الكاذبة بشأنها على مختلف وسائل الإعلام؛ وتزييف المراسلات؛ وفبركة الأدلة؛ واستخدام مذكرات الإحضار أمام هيئات المحلفين الكبرى لإرهاب النشطاء. إن النشطاء اليوم عليهم معرفة ماهية التهديد التي تمثله وكالات تطبيق القانون الفدرالي وما يستخدمونه من تكتيكات فضلاً عن الممارسات الأمنية الأساسية العديدة التي توفر أفضل سبل الحماية.

ثمة العديد من الأدوات المتوفرة في أيدي العملاء الفدراليين لاستهداف النشطاء.
بينما من الضروري أن تعرف وتفهم هذه الأدوات والتكتيكات، من الضروري كذلك أن تعمل على مقاومة هوس الارتياب من مراقبة الحكومة لك أو الخوف من الاختراق، والذي لن يؤدي إلى شيء اللهم إلا إعاقتك وإعاقة منظمتك عن مسيرتها طلباً للتغيير الاجتماعي. فإذا تمكن خوفك من القمع الحكومي من منعك عن التنظيم، فحينئذ فقط يكون العملاء الفدراليين قد انتصروا في المعركة بلا جهد يذكر.

ولقد قام مركز الحقوق الدستورية بإصدار كتيب إذا جاء عميل يطرق الأبواب لتقديم النصيحة إلى النشطاء الذين من المرجح استهدافهم من قبل عملاء المباحث الفدرالية أو غيرهم من المحققين الفدراليين. ومنذ صدوره لأول مرة عام 1989، حقق كتيب إذا جاء عميل يطرق الأبواب رواجاً كبيراً بين مجموعات النشطاء عبر أرجاء الدولة. ويشتمل هذا الدليل على النصيحة الخالدة التي تضمنها الإصدار الأصلي علاوة على تحديثات ثرية تعكس الحالة الراهنة للقانون وأدوات تنفيذه. كما يتضمن هذا الإصدار المحد مناقشة شاملة للتقنية العصرية، بما فيها الهواتف الخلوية والبريد الإلكتروني وتصفح مواقع الإنترنت. أن هذا الدليل من الأحرى اعتباره مصدراً للمعلومات التي تحتاج إليها لحماية نفسك والنشطاء الآخرين من تحريات الحكومة ولتزويدك بالقوة اللازمة لمواصلة الكفاح.

لقد حاولنا جاهدين تقديم إجابات وافية على مجموعة واسعة النطاق من الأسئلة المعنية بالسيناريوهات العديدة التي قد يواجهها الناشط. ونحن نأمل أن يستفيد الأفراد والمجموعات من هذا الكتيب لوضع وإعداد ردود عملية – إذا جاء عميل يطرق الأبواب.

يسلط هذا الكتيب الضوء على ضرورة الحصول على استشارة قانونية في جميع الحالات. حيث لا يتمتع مركز الحقوق الدستورية بالإمكانيات التي تؤهله للتمثيل الجنائي للأفراد.

يوجد في كل ولاية اتحادات محامين والذين في مقدورهم إحالة القضايا إلى محامين، والذين قد يقدم بعضهم خدمات مجانية. إذا كان هناك فرع للتجمع الوطني للمحامين www.nlg.org في مدينتك، فستجدهم دائماً قادرين على إحالة القضايا إلى محامين يتمتعون بالخبرة في القضايا المثارة ضمن صفحات هذا الكتيب.

الزيارات وعمليات التفتيش

هذه هي أهم معلومة يحويها هذا الكتيب: أنت تتمتع بالحق في الالتزام بالصمت، وعادة ما يكون هذا هو أفضل ما تفعله. أن التعديل الخامس لدستور الولايات المتحدة الأمريكية يحميك من إجبارك على الإفصاح عن معلومات تدينك بأي جرم إلى وكالات تطبيق القانون.

إلا أن هذه المقولة من السهل قولها على عكس تنفيذها. فالوكلاء ليسوا إلا محققين مدربين: فلقد تعلموا قوة الإقناع وكيفية إشعار الآخرين بالرعب أو الذنب أو بسوء الخلق لرفضهم طلباتهم للمعلومات. فقد يشير العميل إلى أن عدم رغبتك في التحدث معه إنما يدل على وجود ما تخفيه. وقد يشير كذلك إلى إنه لا يريد منك سوى الإجابة على القليل من الأسئلة ثم يدعك لشأنك. وقد يلجأ العميل أحياناً إلى تهديدك بإصدار مذكرة تفويض قضائي. لا تسمح لتهديدات العميل أو توعده لك بإخافتك أو التلاعب بك. من الأفضل دوماً عدم التحدث بدون وجود محامي. فإذا تحدثت، كل ما ستقوله يمكن استخدامه ضدك وضد آخرين. حتى إذا قلت الحقيقة كاملة، ولم يصدقك العميل، يمكنه تهديدك باتهامك بالكذب على ضابط فدرالي – وهو ما يعتبر جريمة حقيقية. إلى أي عميل يتصل بك عفوياً. عادة ما يقول العملاء إنك لست جزءً من أي تحقيقات، وهو ما قد يكون مخالفاً للواقع. لذا، قل لأي شخص يعرف نفسه بأنه من سلطات تنفيذ القانون إنك ستجعل محاميك يتحدث إليه – ثم توقف عن التحدث إليه. وإن أمكن، احصل على اسم العميل ورقم هاتفه واسم الوكالة التي يعمل بها، وهي جميعاً معلومات يجب أن تتوافر على بطاقة العمل خاصته أو يكون على استعداد لتقديمها إليك. فور أن يغادر العميل أو يغلق خط الهاتف، حاول تدوين أكبر عدد ممكن من التفاصيل حول هذه المداخلة، حيث ستكون هذه المعلومات ذات أهمية بالنسبة إلى المحامي وللآخرين الذين اتصلت بهم وكالة تطبيق القانون. حاول تدوين: اسم العميل و/أو وصفه الشكلي ونوع السيارة التي كان يقودها والأسئلة التي طرحها عليك والتعليقات التي ذكرت أثناء اللقاء؛ وتاريخ إجراء هذه المواجهة وموعدها وموقعها ومعلومات الاتصال بأي شاهد. إن أفضل إجراء يمكنك فعله عادة ما يكون إشراك محامي. فالمحامي يمكنه إسداءك النصح حيال كيفية التقاضي مع حماية حقوقك. كما في وسع المحامي التحدث إلى العميل ومعرفة ما يدور حوله التحقيق والسعي لوضع بعض القيود على موضوع أي استجواب، إلى جانب الحضور أثناء الاستجواب لنصيحتك وحمايتك. أحياناً تكون مكالمة من محامي هي كل ما يلزم حتى يتراجع العميل.

إذا تم استهدافي أو استدعائي من قبل وكالة لتنفيذ القانون، هل يلزم علي التحدث؟

بفضل نصيحة محامي، قد تفكر في إعلام آخرين ممن قد يتأثرون بهذا التحقيق بتلك المواجهة. فإذا علم النشطاء بوجود تحقيق يتم، فقد يكونون أكثر حرصاً على حماية حقوقهم. فالتنظيم الحسن والضغط العام قد يكشف عن محاولات التهديد وحملات التشهير ويحد منها.

1. إبان نشر هذا الكتيب، كان يوجد في الولايات التالية بعض الصيغ من قانون توقف وعرف عن نفسك: ألاباما، أريزونا، أركانساس، كولورادو، ديلاوير، فلوريدا، جورجيا، إيلينوي، إنديانا، كانساس، لويزيانا، ميزوري، مونتانا، نبراسكا، نيفادا، نيو هامشاير، نيو مكسيكو، نيو يورك، ديكوتا الشمالية، أوهايو، رود أيلاند، أوتاه، فيرمونت، ويسكونسن.

ما هي العواقب التي تترتب على تحدثي؟

قد يطرأ عليك موقف ما ترى إنه من الأفضل أن تتحد إلى العميل. فقد تكون ضحية جريمة أو تكون شاهداً على حالات انتهاك للحقوق المدنية يتم التحقيق فيها بواسطة الحكومة الفدرالية. حتى في مثل تلك الظروف، يجب أن يكون لديك محامي حاضراً.

فالمحامي في وسعه ضمان حماية حقوقك مع قيامك بتقديم المعلومات الضرورية فحسب ذات الصلة بحادثة بعينها. كما في مقدور المحامي تجنب مثول الشاهد أمام هيئة المحلفين الكبرى أو على أقل تقدير السيطرة على زمام الأمور أثناء المثول أمام المحكمة بحيث لا يتم انتهاك حقوق أي من الأطراف.

إذا قررت الإجابة على الأسئلة، عليك أن تدرك جيداً أن الكذب على مسؤول حكومي إنما يعتبر جريمة، بل إنه في الواقع من أهم الأسباب التي تدعو إلى عدم التحد إلى العملاء. فمن التكتيكات التقليدية التي تتبعها وكالات تطبيق القانون الفدرالي هو الكشف عن أكبر قدر ممكن من المعلومات حول مشتبه فيه أو حول مجرد شخص ذي أهمية بالنسبة إلى الحكومة. يقوم عقب ذلك العملاء الفدراليين بالتوجه إلى الشخص المعني في أي وقت عادي، كما هو الحال أثناء تناول العشاء أو في محطة الحافلات، ويوجهون إليه أسئلة يعرفون إجاباتها بالفعل.

على سبيل المثال، قد يسألك أحد العملاء ما إذا كنت تعرف شخصاً ما (الذي يعرفون بالفعل إنك على معرفة به) أو قد يسألونك عما إذا كنت حاضراً في حد ما (الذي يعرفون إنك كنت حاضراً فيه بالفعل). فإذا انكرت بدافع الغريزة وقلت "لا"، فإن هذا يعد جناية فدرالية يعاقب عليها القانون بالسجن لمدة تتراوح من خمس إلى ثمان سنوات. إن أكثر ما يثير الرهبة في ذلك التكتيك التحقيقي أن العديد من الأشخاص سوف يجيبون على الفور بتلقائية بلا علي أي سؤال نتيجة لخوفهم أو لتوترهم. ولذا، كثيراً ما يلجأ العملاء الفدراليون إلى هذا التكتيك في جميع أنواع التحقيقات، كما تم استخدامه مؤخراً لاستهداف النشطاء وتحويلهم إلى مخبرين ضد زملائهم السابقين.

إن الكذب على مسؤول فدرالي لهو جريمة فدرالية وهي تسري فقط على الأسئلة التي يتم توجيهها من قبل عملاء فدراليين. ومع ذلك، عليك الانتباه إلى أن الوكلاء المحليين والحكوميين، مثل أعضاء القوة المشتركة لمكافحة الإرهاب التابعة للمدينة، يعتبرون كذلك عملاء "فدراليين". وبالمثل، ثمة بعض الدول التي لديها جرائم مشابهة بشأن الكذب على مسؤول حكومي. ومن ثم، فإن الاختيار الأمن هو عدم التحد إلى سلطات تطبيق القانون.
إذا بدأت الإجابة على الأسئلة، يمكنك رفض متابعة الإجابة في أي وقت.

مذكرات التفتيش

مذكرة التفتيش عبارة عن أمر محكمة يصرح لسلطات تطبيق القانون تفتيش موقع محدد واحتجاز الأدلة.

يهدف التعديل الخامس إلى حماية الأشخاص ضد عمليات التفتيش غير المعقولة. إلا في حالة تطبيق استثناء، يطلب من عملاء تطبيق القانون الحصول على مذكرة تفتيش لإجراء عملية تفتيش. هذا ويلزم دعم مذكرات التفتيش بسبب مرجح، إلى جانب حقائق يقسم على صحتها مقدم طلب المذكرة. يلزم أن تكون مذكرة التفتيش معنية بالمنطقة المحددة التي سيتم تفتيشها والأغراض التي سيتم البحث عنها. كذلك يجب أن يقوم قاض بالتوقيع على مذكرة التفتيش وأن يتم تأريخها بتاريخ حديث (في غضون أسبوعين) مع ذكر العنوان الصحيح للموقع. يقصد بالسبب المرجح ضرورة وجود وقائع تفيد بوجود دليل على إنه من الأرجح أن يتم اكتشاف جريمة في المنطقة المطلوب تفتيشها. يجب أن يستند السبب المرجح على حقائق – فالحدس وحده لا يكفي.

مسلحين بمذكرة التفتيش، يحق لعملاء تطبيق القانون تفتيش ممتلكاتك. فإذا لم تسمح لهم بالدخول، فسوف يلجئون على الأرجح إلى استعمال القوة لتنفيذ التفتيش.

تعرف على أدواتهم

ماذا إذا طلب أحد العملاء تفتيش منزلي أو شقتي أو مكتبي؟

لا تسمح لعميل تطبيق القانون على الإطلاق بتفتيشك شخصياً أو تفتيش ممتلكاتك بدون مذكرة تفتيش. فيلزم على عملاء تطبيق القانون الحصول على مذكرة تفتيش ليحق لهم تفتيش ممتلكاتك إلا في حالات معينة محدودة. أنت غير مسموح لك قانوناً إلا بالسماح لعملاء تطبيق القانون بالدخول إلى منزلك أو مكتبك أو أي مكان آخر خاص بك إذا كانت لديهم مذكرة.

قد يقوم العملاء بتفتيش منزلك بدون مذكرة إذا سمحت لهم بذلك، وهم مدربون على طلب موافقتك لضمان عمليات تفتيش أقل. احذر من الأسئلة التي تم وضعها خصيصاً لحثك على الموافقة على التفتيش، فقد تبدو هذه الأسئلة بريئة مثل "هل تمانع في أن أدخل؟" فإن السماح للعميل بالدخول إلى منزلك قد يمثل موافقة على تفتيش المكان بأكمله.

شرعاً، تعد الإجابة الأفضل لطلب التفتيش هي "أنا لا أوافق على التفتيش". قل ذلك بصوت مرتفع وبفخر بحيث يمكن لأي شاهد سماع صوتك.

ماذا إذا لم أكن متواجداً وطلب أحد العملاء من زميلي في السكن تفتيش ممتلكاتي؟

يمكن لزميل السكن الموافقة على تفتيش المكان الشائع المشترك ومكانه الخاص. بينما لا يجوز لزميل السكن الموافقة على تفتيش المكان الخاص بشخص آخر في منزل مشترك أو شقة مشتركة. وبكلمات أخرى، يمكن لزميل السكن الموافقة على تفتيش مطبخك أو غرفة المعيشة أو الحمام المشترك، لكنه لا يجوز له الموافقة على تفتيش غرفة نومك الخاصة، إلا إذا كان يشارككَ إياها أو إذا كانت تستخدم كمكان مشترك على نحو ما.

يمكن للأزواج/الزوجات الموافقة على تفتيش الغرف الخاصة للشركاء حيث يعتبرون أنهم يمتلكون سلطة مشتركة على جميع أرجاء المنزل. وبالمثل، يحق للوالدين الموافقة على تفتيش الأماكن الخاصة بأطفالهم. وإجمالاً للقول، إذا كنت تشارك غرفة نوم مع زميل سكن أو شريك، يمكنهم الموافقة على تفتيش ذلك المكان.

للحماية ضد عمليات التفتيش غير المرغوبة، احرص على أن يظل المكان الخاص بك خاصاً. فإذا سمحت لزملاء السكن بالتمتع بحرية الدخول والسيطرة على المكان الخاص، سيجوز لهم الموافقة على تفتيش هذا المكان. لذا عليك إخبار زملاء السكن وزملاء المكتب وأي شخص تتشارك معه في أي مكان ألا يوافقوا مطلقاً على إجراء عمليات تفتيش لأي مكان، ولا سيما مكانك الخاص.

هل يمكن للعملاء تفتيش نفايتي؟

فور أن تضع النفايات خارج منزلك، يجوز للعملاء تفتيشها دون مذكرة أو أي قيد قانوني آخر. فلقد توصلت المحاكم إلى عدم وجود أي حق بالخصوصية في قمامتك حيث إنك تسلمها إلى الجمهور العام. لذا، قم بتمزيق أي مستندات حساسة أو قم بتدميرها على أي نحو آخر قبل التخلص منها.

ماذا إذا هددني أحد العملاء بإصدار مذكرة مثول أمام المحكمة أو مذكرة إحضار إذا لم أتحدث أو أوافق على التفتيش؟

لا تخش من تهديدات العميل بالحصول على مذكرة أو أمر إحضار، فهذه واحدة من أقدم الحيل التقليدية. فإذا كان من السهل عليه إحضار واحد، لم يكن ليهدر الوقت في محاولة الحصول على تعاونك التطوعي. مرة أخرى، كل ما عليك هو تأكيد عدم موافقتك على أي تفتيش وإنك لن تتكلم دون وجود محاميك.

ماذا إذا ادعى أحد العملاء وجود إذن تفتيش معه؟

إذا ادعى عميل أن بحوزته مذكرة، اطلب منه رؤيتها. يجب أن تكون مشابهة لمذكرة التفتيش البسيطة المصورة هنا ويجب أن تكون موقعة من قاض لتكون صالحة. كذلك يجب أن تكون مذكرة التفتيش محدد بها المكان الذي سيتم تفتيشه والشيء (الأشياء) التي سيتم التفتيش عنها. فلا توافق على قيام العميل بتفتيش أي أماكن غير مضمنة تحديداً في مذكرة التفتيش.

إن مجرد وجود مذكرة تفتيش مع العميل لا يعني إنه يلزم عليك الإجابة على أية أسئلة. فحافظ على حقك في الالتزام بالصمت أثناء التفتيش ـ أعلن بوضوح عن عزمك هذا إذا كالبك العميل بالإجابة على أية أسئلة.

ما هي الحقوق التي أتمتع بها وتخولني الحق في منع العملاء من تفتيش سيارتي؟

تتمتع سلطات تنفيذ القانون بسلطات واسعة النطاق على صعيد تفتيش السيارات بدون مذكرة. فإذا كان يتوفر لدى العميل سبب مرجح للاعتقاد بوجود دليل جريمة ما داخل أي سيارة، يجوز للعميل، بدون مذكرة، تفتيش تلك السيارة وأي حاوية داخل السيارة يكون حجمها مناسب لاحتواء الغرض الذي لديه سبب مرجح للبحث عنه. على سبيل المثال، إذا كان العميل لديه سبب مرجح للاعتقاد بأنك قد سرقت جهاز تلفزيون كبير الحجم، يمكنه تفتيش حقيبة السيارة، بينما لا يحق له تفتيش صندوق القفازات أو صندوق عدة صغير موجود داخل السيارة. إذا كان لديه سبب مرجح لتفتيش حاوية تم وضعها حديثاً داخل السيارة، فلا يجوز له تفتيش سوى هذه الحاوية فحسب.

إذا تم إلقاء القبض عليك واحتجاز سيارتك، يجوز لسلطات تنفيذ القانون إجراء تفتيش لجرد محتويات السيارة بدون مذكرة. وهو ما يعني إنه يحق للشرطة تفتيش سيارتك لتسجيل ما يوجد بداخلها، كما يحق لهم استخدام كل ما يوجد بداخلها ضدك لأي سبب. يجب أن تتم عمليات التفتيش للجرد وفقاً للإجراءات المحلية المقررة، ولا يجوز للشرطة استخدام تفتيش الجرد كذريعة لإجراء تفتيش بدون مذكرة.

ما الذي يتعين علي فعله إذا اكتشفت اقتحام أحدهم لمكتبي أو منزلي وكنت أشك في أن الدافع وراء ذلك هو تجميع المعلومات الاستخباراتية؟

إذا تم اقتحام منزلك أو مكتبك، أو إذا تم توجيه أية تهديدات لك أو لمنظمتك أو لأحد زملائك في العمل، قم بمشاركة تلك المعلومات مع كل من له صلة بهذا الأمر واتخذ خطوات فورية لزيادة الأمن الشخصي وأمن المكتب. يتعين عليك الاتصال بمحامي على الفور.

عمليات تفتيش "التسلل واختلاس النظر"

تتيح عمليات تفتيش "التسلل واختلاس النظر" للحكومة، بموجب موافقة سرية من إحدى المحاكم، إجراء عمليات تفتيش ومراقبة دون إخطار الشخص محل التفتيش. وحيث إن عمليات تفتيش التسلل واختلاس النظر من المفترض إجراؤها على نحو سري، فعادة ما تتم عن طريق اقتحام الأماكن ودخولها.

عادة ما يلزم على العميل المثول أمام قاض موضحاً الأسباب المرجحة التي تدفعه إلى طلب مذكرة تفتيش. أمام محكمة مراقبة المخابرات الأجنبية، على الرغم من ذلك، يمكن أن يحصل العملاء على تصريح بإجراء تفتيش بالتسلل واختلاس النظر إذا تمكنوا من البرهان على أن التفتيش سوف يوفر معلومات مخابرات أجنبية. كما ليس بالضرورة أن يكون جميع معلومات المخبرات الأجنبية هو الدافع الرئيسي وراء التفتيش، بل يجب أن يكون فقط سبباً مهماً للتفتيش. وهو ما يعني إنه يمكن للعميل الحصول على تصريح بتفتيش منزلك لجمع الأدلة على أعمال إجرامية طالما كان جمع معلومات المخابرات الأجنبية من ضمن أهداف التفتيش.

بينما تم تصميم عمليات تفتيش التسلل واختلاس النظر بهدف جمع معلومات المخابرات الأجنبية، سمحت معظم المحاكم باستخدام أدلة ومعلومات تم الحصول بواسطة عمليات تفتيش التسلل واختلاس النظر بهدف استخدامها في الدعاوى الجنائية.

⚠ تعرف على أدواتهم

ماذا أفعل في حالة حضور العملاء ومعهم تصريح بالاعتقال؟

تصريح الاعتقال هو أداة تستخدمها الشرطة وغيرها من الوكالات المعنية بتطبيق القوانين لتدخل إلى منزلك وتنفذ أمر الاعتقال. ويعد واحداً من المنافذ المتعددة لمتطلبات تصاريح التفتيش هو أنه بمجرد تواجد العملاء داخل منزلك، حتى ولو لم يكن معهم سوى تصريح بالاعتقال، فلديهم مهلة كبيرة بإجراء التفتيش. ويمكنهم القيام بتفتيش فوري للمناطق المحيطة بك دون حيازتهم لإذن بالتفتيش. كما يحق لعملاء تطبيق القانون إجراء "تفتيش وقائي" شامل للمنزل إذا كان لديهم اعتقاد بإمكانية تواجد شخص خطِر فيه.

في حالة قدوم عملاء تنفيذ القانون إلى منزلك (أو أي مكان آخر) ومعهم تصريح بالاعتقال، فأفضل ما يمكنك فعله هو الخروج وتسليم نفسك. وقم بإغلاق الباب خلفك، إذا كان فعل ذلك آمناً. لو كان عملاء تنفيذ القانون يملكون تصريحاً بالقبض عليك، فسيقومون باعتقالك. لا تمنحهم الفرصة لقيامهم بتفتيش منزلك بدون تصريحاً بذلك.

مذكـــــرة إحضـــــار

تصريح الاعتقال هو أمر من المحكمة يسمح لعملاء تنفيذ القانون باعتقال شخص محدد. يتم إصدار تصريح الاعتقال والتوقيع عليه من قبل المحكمة بناءً على التقدم بطلب مشفوع بالقسم من قبل هيئات تنفيذ القانون يؤكد أنه هناك سبب مقنع بأن هناك جريمة قد وقعت، وأن الفرد أو الأشخاص الواردة أسمائهم في التصريح هم من ارتكبوها.

وبوجه عام، فلا تحتاج الشرطة أو أية جهة أخرى لتنفيذ القانون إلى الحصول على تصريح بالاعتقال لتنفيذ أمر القبض. فبمجرد تأكدهم من ارتكاب الجريمة، يمكنهم القيام بالاعتقال.

وهناك استثنائان شائعان لهذه القاعدة. الأول، يحتاج عملاء تنفيذ القانون في معظم الولايات وليس جميعها، للحصول على تصريح بالاعتقال للجنايات التي لم يشهدوها بأنفسهم. من المهم أن تلاحظ، أنه يحق لعملاء تنفيذ القانون، الاعتقال بتهمة ارتكاب جريمة دون الحصول على تصريح. والثاني، تحتاج هيئات تنفيذ القانون بوجه عام إلى حيازة إذن بالاعتقال عند اعتقالك من المنزل. وعلى أي حال، فمن الممكن أن تقوم جهات تنفيذ القانون باعتقالك من منزلك دون تصريح بالاعتقال، في حالة توقعهم لأن تقوم بتدمير الأدلة أو أنهم كانوا يطاردونك إلى أن اختبأت في منزلك أو منزل أي شخص آخر.

⚠ تعرف على أدواتهم

ما الذي يتعين علي فعله إذا تلقيت مذكرة استدعاء؟

يجب أن تسعى إلى إسقاط مذكرة الاستدعاء تلك قبل تاريخ المثول الموضح فيها، لكن حتى في مذكرات الاستدعاء التي تتطلب الحضور الفوري بأمر الدولة لا يمكن تنفيذها إلا بأمر قضائي.

لو ظهر شخص ما عند بابك وحاول تسليمك مذكرة استدعاء، خذها فحسب. لا تسمح لهذا الشخص بالدخول، ولا تجب على أية أسئلة، ولا توافق على قيامه بالتفتيش. فمذكرة الاستدعاء لا تمنح العميل الحق في اتخاذ أي إجراء فوري.

يجب أن تستعين بخدمات محامي ليساعدك في إسقاط مذكرة الاستدعاء. وعلى النقيض من ذلك، لو علمت بأنه قد تم استدعاء طرف خارجي لمعلومات بشأنك – فليس من المهم أن توجه مذكرة الاستدعاء مباشرة إليك.

أوامـــر الإحضـــار

مذكرة الاستدعاء هي أمر يصدر من السلطات الحكومية يطالب شخص ما بتسليم أدلة مادية كالمستندات، أو بالشهادة في المحكمة.

من السهل جداً الحصول على مذكرات الاستدعاء. عادة ما يتم ملؤها من قبل موظف حكومي، أو كاتب المحكمة، أو حتى من المحامي الخاص.

لا تحتاج مذكرات الاستدعاء إلى أن يتم عرضها على القضاء قبل إصدارها. كما أن الأدلة التي يجب تقديمها للحصول على مذكرة استدعاء قليلة جداً؛ حيث إنه يتم إصدار مذكرات الاستدعاء في حال كان هناك أي سبب مقنع أن ما سيتم تقديمه من أدلة مادية أو شهادة أمام المحكمة ستوفر معلومات هامة متعلقة بالقضية التي يتم التحقيق فيها.

السهولة التي يتم بها إصدار مذكرات الاستدعاء جعلت منها أداة قوية جداً، على خلاف أذون التفتيش وغيرها من الأدوات الحكومية الأخرى، والتي يمكن تداولها أمام القضاء قبل المثول. في حالة تسلمك لمذكرة استدعاء، يمكنك التحرك في إجراءات "إسقاط" مذكرة الاستدعاء إذا كانت عامة جداً أو مبالغ فيها أو تسعى للحصول على مادة محمية بموجب القانون، بما في ذلك المواد المحمية بموجب الدستور. بمجرد أن يتم إسقاط مذكرة الاستدعاء، فلن يكون هناك حاجة إلى المستندات أو شهادة الشخص المستلم.

وتتشكل خطورة مذكرات الاستدعاء في أن جهة تنفيذ القانون قد تقوم باستدعاء أطراف خارجية أخرى والذين قد يكون لديهم معلومات عنك. قد تقوم الحكومة باستدعاء أفراد آخرين بناءً على الرسائل الإلكترونية التي قد أرسلتها لهم. لأن هؤلاء الأطراف الخارجيين ليس لديهم نفس الرغبة التي لديك في إسقاط مذكرة الاستدعاء، ويرغبون بشكل أكبر في الاستجابة لمذكرة الاستدعاء دون منازعة.

⚠ تعرف على أدواتهم

الاختراق والمراقبة البشرية

إن استخدام العملاء المتخفيين والمخبرين السريين أمر لا مفر منه في التحقيقات التي تجريها وكالات تنفيذ القانون بموجب القوانين الحديثة. تمنح القدرة على زرع عملاء متخفيين أو مخبرين في الحركات التقدمية أو المنظمات، لهيئات تنفيذ القانون نوع من صلاحية الوصول إلى المعلومات التي لا يمكن تقريباً الوصول إليها بالطرق الأخرى. الاختراق هو وسيلة مفيدة جداً في الحصول على المعلومات السرية الخاصة بأنشطة الأفراد الخاصة، وتوفر لوكالات تنفيذ القانون القدر الكافي من المعلومات اللازمة لإتمام التحقيقات.

يقدم المخبرون والعملاء المتخفون تقاريرهم إلى هيئات تنفيذ القانون عن الأفراد المشاركين في الحركة وجوانبها التكتيكية والتنفيذية. من الممكن أن يعملوا أيضاً على توجيه أو تشجيع المشاركين على ارتكاب أفعال غير قانونية في ظل محاولتهم لاعتقالهم. وقد قررت المحكمة بشكل عام بحظر إفشاء اسم المخبر بموجب قوانين الشرطة إلا في حالة كان ذلك ضرورياً لاستخدام الدفاع في المحكمة الجنائية، ولهذا فمن النادر أن يتم استدعاء المخبرين للشهادة في المحكمة، ذلك للسماح لهم بالتصرف بقدر ضئيل من تحمل المسؤولية.

المخبـــــرون

المخبرون هم أفراد غير موظفين بصفتهم عملاء تنفيذ قانون، يقومون بتزويد وكالات تنفيذ القانون بالمعلومات، وعادة ما يكون ذلك مقابل الأموال. عادة ما يكون المخبر قد شارك سابقاً – وعلى دارية جيدة – في الحركات أو المؤسسات التي تتحرى عنها الوكالة.

⚠ تعرف على أدواتهم

العمـــلاء المتخفـــون

العميل المتخفي هو ضابط في هيئات تنفيذ القانون والذي يستخدم اسماً مستعاراً وهوية مزيفة ليخترق حركة ما أو منظمة بغرض جمع المعلومات أو الأدلة. في حالات الاختراق السياسي، عادة ما يتخذ العميل موقف المتعاطف مع المنظمة، بغرض كسب ثقة الأعضاء الرئيسيين فيها ومن ثم يستخدم هذه الصلاحية في جمع المعلومات الخاصة ورفعها إلى الوكالة المعنية بالتحقيق. قد يكون هناك هدف ثانوي آخر وهو التمهيد لإجراء تحقيق مستقل آخر. عادة ما يقوم العملاء المتخفون باختلاق قصة للتغطية كما هو وراد بالتفصيل في متطلبات المهمة بالإضافة إلى السيرة الذاتية والمظهر الذي يناسب قصة التغطية على الأنشطة الجارية والماضية.

⚠ تعرف على أدواتهم

الشهـــود المتعـــاونون

هناك تشابه بين المخبرين والشهود المتعاونين، فيما عدا أن الشهود المتعاونين عادة ما يوافقون على "الوشاية" أو "الانقلاب" بعد أن يتم تهديدهم بتعرضهم للمحاكمة. يدلي الشهود المتعاونون بشهاداتهم أمام المحكمة مقابل إسقاط كافة التهم ضدهم لو كان هناك أي منها.

عادة ما تقوم وكالات تنفيذ القانون بتجنيد المخبرين والشهود المتعاونين من فئة الأفراد النشطين فعلياً داخل الحركات أو التنظيمات المستهدفة. في الغالب تقوم وكالات تنفيذ القانون بتهديد هؤلاء الأفراد بتوقيع عقوبات مشددة تصل بالسجن، أو عرض بعدم توجيه التهم إليهم مقابل وعد منهم بالتبليغ عن غيرهم في الحركة.

وعلى الجانب الآخر، فإن العملاء المتخفين يستخدمون هويات مزيفة منذ بداية تدخلهم في أي حركة أو تنظيم.

⚠ تعرف على أدواتهم

هل هناك حدود لما يمكن للعملاء والمخبرين المتخفيين القيام به؟

لا توجد قوانين محددة تحكم أو تحد من استخدامات هيئات تنفيذ القانون للعملاء المتخفين أو المخبرين، وما ليس هناك أية قيود على أنواع جرائم الاختراق المستخدمة في التحقيقات. على خلاف الدول الأخرى، فإن اللجوء للممارسات المتخفية لا يحتاج إلى تصريح، فلا يكون ضباط تنفيذ القانون بحاجة إلى لإظهار أنه يتم استخدام مخبر أو عميل متخفي في تحقيقات بعينها. ولا يحكم استخدام المباحث الفيدرالية للعملاء المتخفين سوى الإرشادات الداخلية العامة والتي تم وضعها بناءً على نتائج التقرير النهائي الذي أعدة مجلس الشيوخ لما يتعلق بدراسة أنشطة الحكومة المرتبطة بالممارسات الاستخباراتية (1976). ذكر التقرير تفاصيل حول برنامج العمليات المموهة (COINTELPRO) التابع للمباحث الفيدرالية والذي يتمتع بسمعة سيئة، على العمليات في الفترة ما بين 1956 حتى 1971 والتي استهدفت نشطاء وتنظيمات منها الدكتور مارتين لوثر كينج، و جي آر، وتنظيم النمر الأسود.

وكاستجابة لذلك التقرير، قام المدعي العام الأمريكي بسن قوانين داخلية لتحكم العمليات السرية للمباحث الفيدرالية ونظمت استخدام العملاء والمخبرين المتخفين. وفي الوقت الذي كانت فيه تلك الإرشادات قوية في بدايتها، فقد أخذت تضعف شيئاً فشيئاً مع تعاقب الإدارات. ففي الوقت الحالي تسمح هذه الإرشادات باستخدام ممارسات عدوانية والتي قد صممت في الأساس لمنعها.علاوة على ذلك فلم تكن تلك الإرشادات قابلة للتطبيق في المحكمة، لهذا فهي لا توفر سوى حماية محدودة من الاختراق والمراقبة. بمعنى آخر، لو قام عميل بجمع أدلة بما يخالف تشريعات المباحث الفيدرالية، فتظل إمكانية استخدام هذه الأدلة في المحكمة.

ما هو الإيقاع في الشرك؟

يعتبر عدم الإيقاع في الشرك هو أكثر القيود المفروضة على العملاء والمخبرين المتخفين. الإيقاع في الشرك هو أن يقوم العميل أو المخبر المتخفي في زراعة أو تحفيز الفرد على فكرة ارتكاب جريمة لم يكن ليرغب في ارتكابها ومن ثم يشجعه على ارتكابها بغرض محاكمته. تنظر المحاكم في نصب الشراك بتمعن، كما أنها تمنح مساحة كبيرة من الحرية للمخبرين والعملاء المتخفين الذين يقترحون أو يشجعون على ارتكاب الأفعال غير القانونية.

بينما تتباين الاستثناءات الدفاعية ضد الوقوع في الشرك من ولاية إلى أخرى، فإنها في مجملها تعتبر دفاعاً غير فعال إذا قام العميل المتخفي بعرض الجريمة فقط. في بعض الولايات لا يعتبر الإيقاع في الشرك دفاعاً ذا قيمة لو رأت هيئة المحلفين أن الفرد لم يكن ليقبل على ارتكاب الجريمة. وفي الولايات الأخرى، لا يعتبر الإيقاع في الشرك دفاعاً على الإطلاق لو كانت الجريمة تنطوي على "التهديد أو التسبب في إيذاء جسدي" ولهذه الأسباب لا يمكن الاعتماد على توافر دفاع الإيقاع في الشرك.

ما هي الحدود الدستورية لسلطات العميل التي تخوله الاختراق؟

يسمح بشكل عام للمخبرين والعملاء المتخفين بحضور الاجتماعات العامة، بما في ذلك التي تعقد في دور العبادة. وقد وجدت المحكمة في بعض الأوقات انتهاكات للدستور من قبل هيئات تنفيذ القانون حين تدخلها في قدرة المجموعات على ممارسة حقوق حرية التعبير والتفكير. وبالمثل، فقد وجدت المحكمة انتهاكاً للمادة الأولى من الدستور من قبل هيئات تنفيذ القانون عندما تقوم بجمع ونشر معلومات عن التنظيمات أو النشطاء.

ولم تجد المحكمة خرقاً للدستور في تسبب عملاء تنفيذ القانون في تعكير أجواء الاجتماعات العامة قد وجدت المحاكم بشكل روتيني أنه لا يوجد خرق للمادة الرابعة من الدستور في قيام العملاء المتخفين بتسجيل المحادثات سرياً، حيث إنه يحول دون عمليات التفتيش والاعتقال غير المبررة. كما أن المحاكم قررت أن قيام المخبرين أو العملاء المتخفين بتسجيل المحادثات لا يعد خرقاً للمادة الخامسة من الدستور حيث إنها تحول دون الاعتراف بارتكاب الجريمة. وبالمثل، لو قمت بدعوة أحد العملاء المتخفين إلى منزلك أو أي من الأماكن الخاصة دون علم منك، فتعتبر المحكمة ذلك بمثابة "موافقة" منك على أن يقوم العميل بالتفتيش. لو شاهد هذا العميل ما قد يعد سبباً محتملاً لجريمة، فمن حقه أن يقوم باستدعاء عملاء تنفيذ الآخرين لمشاركته في عملية التفتيش بناءً على الموافقة التي منحتها لهذا العميل المتخفي.

وقد نزعت بعض المحاكم إلى تطبيق نفس النتيجة على المواقف التي يقوم فيها الهدف بغير علم بدعوة احد المخبرين إلى دخول منزله.

كيف يمكنني تحديد أدلة الاختراق؟

هناك عدة طرق للتعرف على الدخيل. قد يتطوع العميل أو المخبر لتنفيذ الأنشطة التي تمنحه صلاحية الوصول إلى المستندات الهامة أو اجتماعات المجموعة، مثل المستندات المالية، وقوائم الأعضاء، والمذكرات والملفات السرية.

وقد يعمل المخبرون والعملاء المتخفون على تشجيع ارتكاب الأفعال المخالفة للقانون ومجادلة من يخالفهم الرأي واتهامه بالجـ . وعادة ما يقوم العملاء والمخبرون باتهام غيرهم بأنهم عملاء أو مخبرون، وبهذا يقومون بإبعادهم عن بؤرة الاهتمام وتشتيت المجموعة عن أعمالها.
قد لا يكون هناك مصدر دخل واضح للعميل أو المخبر المتخفي عن فترة من الزمن، أو قد يكون لديه الكثير من الأموال التي قد يتقاضاها من عمله.
حاول الحصول على معلومات تخص الشخص المشكوك في كونه عميلاً أو مخبراً. تحرى بالتعاون من المنظمة عن الأماكن التي كان يقطنها العميل فيما مضى للتحقق ما إذا كان أحد سيتعرف عليه أم لا.

لترى ما يمكنك التوصل إليه عبر الانترنت، أو من السجلات العامة كتقارير الأرصدة، أو البطاقات الانتخابية والرهونات التي تحتوي على بيانات وفيرة، بما في ذلك العناوين الحالية والسابقة. كما أنه بإمكانك مراجعة قوائم حديثي التخرج من أكاديميات الشرطة المحلية حين توافرها؛ لكن، عليك أن تتذكر أن الشخص المشكوك فيه قد لا يكون مستخدماً لاسمه الحقيقي.
ليس من الضروري أن يكون الشخص الذي تنطبق عليه هذه المواصفات يعمل كمخبر أو عميل متخفي. فعليك توخي الحذر ولا تتهم أي شخص بكونه عميلاً أو مخبراً ما لم يكن لديك الدليل القاطع على ذلك.

ما هي الإجراءات الوقائية التي يمكنني اتخاذها لحماية منظمتي؟

احتفظ بسجل لكل عمليات المراقبة أو التلاعب سواء كانت مؤكدة أو مشكوك فيها. قم بتدوين التواريخ، والأماكن، والحضور؛ ووصفاً تفصيلياً لكل شيء يحد ؛ وأية تعليقات تفسر محتوى التجربة ووصفاً تفصيلياً لتأثير هذا الحد على الأفراد أو المنظمة. قم بعقد اجتماع لمناقشة عمليات التجسس والمضايقات، وحدد ما إذا كان أي من أعضائك قد تعرض لمضايقات أو لاحظ أنشطة مراقبة والتي يبدو أنها موجهه إلى أنشطة المنظمة. قم بمراجعة الأنشطة المشبوهة أو الصعوبات التي تواجه المجموعة، وحاول تحديد ما إذا كان هناك من شارك في هذه الأحدا سواء كان فرداً واحداً أو أكثر.

ربما تضطر إلى تقديم طلبات بتطبيق قانون حرية النشر لحماية منظمتك من مثل تلك الوكالات كالمباحث الفيدرالية، وزارة الأمن الوطني، ودائرة المشروبات الكحولية والتبغ والأسلحة النارية، وغيرها من الوكالات الفيدرالية. وتقدم بطلب مماثل إلى وكالات تنفيذ القانون المحلية والدولية مطالباً بتطبيق قوانين حرية المعلومات المتبعة في ولايتك. والأكثر أهمية، هو ألا تسمح بأن يسيطر الرعب من الاختراق على منظمتك حتى يصيبها بالشلل. قد يكون الرعب مدمراً بنفس قدر الاختراق.

المراقبة الإلكترونية

يتناول هذا الفصل الطرق التي يستخدمها العملاء في زرع أجهزة التصنت مُراقبة المُكالمات الهاتفية واستخدام الإنترنت خلال تحقيقاتهم. وحيث إن حياتنا أصبحت تتسم بالرقمية في كافة الأوقات، فمن ثم تزايد استخدام العملاء للمُراقبة الإلكترونية في جمع المعلومات. ومع الأسف، محاولات المحاكم والسلطات القانونية لمواكبة وتيرة التكنولوجيا عادة ما تبوء بالفشل، الأمر الذي يؤدي في كثير من الأحيان إلى تضاءل أو انطماس حماية الخصوصية للحصول على أحد التقنيات.

تُقيد قاعدة بحكم التجربة بأنه: "كلما كانت وسائل الاتصال أقدم، كلما زادت الحماية التي يمنحها لها القانون". وكما صرح السيد/إليوت سبيتزر عندما يشغل منصب النائب العام بولاية نيويورك: "إياك والكتابة إذا كان بمقدورك التحد . وإياك والتحد إذا كان بمقدورك الإيماء. ولا تضع أي شيء في بريد إلكتروني لأن ذلك هو الموت بعينه. أنت تمنح المدّعون كل دليل نحتاج إليه".

الاتصالات الهاتفية

يُمكن اعتراض المُحادثات الهاتفية باستخدام العديد من الوسائل المختلفة ابتداءً من المراقبة إلى التصنت المتنقل إلى جهاز تسجيل الأرقام ووصولاً إلى أجهزة الاعتراض والتعقب. تُعد طرق المراقبة الهاتفية مُفصلة ومُعقدة. ولا يسعنا سوى ذكر لمحة عامة عنها فحسب. الدرس بسيط للغاية – توخ الحذر فيما تتلفظ به عبر الهاتف.

متى يجوز للحكومة التصنت على مكالماتي الهاتفية؟

عادةً ما تحتاج الحكومة إلى تفويض خاص يُطلق عليه "أمر تصنت من الباب الثالث" للتمكن من التصنت على هاتفك. غير أن الحكومة باستطاعتها أيضًا التصنت على هاتفك دون أمر قضائي لمدة 48 ساعة وذلك في حالات الطوارئ التي تنطوي على موت فوري أو إصابة بالغة الخطورة أو قضية أمن قومي أو أية أنشطة تتسم بطابع الجريمة المنظمة. يُمكن للحكومة بعد ذلك السعي للحصول على أمر قضائي لترخيص المراقبة المستمرة التي تشتمل على عمليات التصنت سالفة الذكر.

أوامر التصنت من الباب الثالث

أوامر تصنت الباب الثالث هيّ التفويضات التي يتم استخدامها لاعتراض ومراقبة اتصالاتكَ الهاتفية. بالإضافة إلى التعديل الرابع للحماية والذي يتطلب أمر قضائي بالتفتيش في مُعظم عمليات التفتيش، قام الكونجرس بتوفير حماية إضافية بشأن الاتصال الشفوي في الباب الثالث من القانون الجامع لمكافحة الجريمة وتأمين الشوارع رقم 1968. وقد صدرت هذه الحماية ردًا على النتائج التي توصل إليها الكونجرس من قبل مكتب التحقيقات الفدرالي في الستينات بشأن المراقبة المُسيئة وغير الشرعية واسعة الانتشار (انظر "هل هناك حدود لما يمكن للعملاء والمخبرين المتخفيين القيام به؟").

يجب على الوكلاء تصنيف تطبيق الباب الثالث المطول والذي يشمل: حقائق بشأن الجرائم التي تم ارتكابها أو التي على وشك أن تُرتكب؛ والمكان الذي سيتم منه اعتراض الاتصالات؛ والاتصالات المعنية الواجب اعتراضها؛ وما إذا كان هناك أدوات تحقيق أخرى مُستخدمة ولم تكن كافية أو غيرها من الأدوات التي لا تفي بالغرض أو تُمثل خطورة من حيث التطبيق؛ والإطار الزمني للاعتراض؛ وبيان بجميع تطبيقات التصنت السابقة بشأن نفس الهدف أو المكان.

لإصدار أمر تصنت من الباب الثالث، يتعين على القاضي تحري ما يلي: السبب المُرجح بأن يكون الهدف قد ارتكب جريمة يشملها الباب الثالث؛ وأن تكون الاتصالات التي تتعلق بهذه الجريمة سيتم الحصول عليها عن طريق الاعتراض؛ وأن تكون المرافق التي سيتم من خلالها اعتراض الاتصالات تُستخدم في الاتصال مع الجريمة.

في المقام الأول، الباب الثالث يسمح بمراقبة فئة ضئيلة فحسب من الجرائم الخطيرة. وعلى مر السنين، قام الكونجرس بإضافة المزيد والمزيد من الجرائم إلى الباب الثالث. وفي الوقت الحالي، القانون يشمل المئات من الجرائم، بما في ذلك بعض الفئات العريضة مثل الجرائم التي تنطوي على المُخدرات أو أعمال الشغب أو الفُحش أو التدخل في التجارة. التفسيرات واسعة النطاق لهذه الجرائم تسمح بمراقبة العديد من أنماط مذهب الفاعلية.

⚠ تعرف على أدواتهم

أوامر التصنت من الباب الثالث (تـــابع ...)

قد تستمر أوامر التصنت من الباب الثالث في البداية لمدة تصل إلى 30 يومًا. يُمكن لهيئات تنفيذ القانون الرجوع إلى القاضي بغرض تمديد تلك الفترة. يُمكن للقاضي إصدار أمر للحكومة بالكشف عن قائمة الاتصالات المعترضة لأهداف التصنت وذلك بعد انتهاء أمر التصنت من الباب الثالث. هذه القائمة المذكورة سلفًا تُخطر الأهداف بالفترة الزمنية للتصنت وما إذا كانت الاتصالات قد تم اعتراضها بالفعل. غير أنه يحق للقاضي اتخاذ القرار بعدم المطالبة بإصدار مثل هذه القائمة.

على وجه العموم، يُعد محاولة الحصول على أمر التصنت من الممارسات النادرة لهيئات تنفيذ القانون، بيد أنهم يحصلون عليها بشكل دائم تقريبًا عند طلبهم لها. على سبيل المثال، في عام 2007، تم تقديم 2208 طلب فقط للحصول على أوامر التصنت إلى محاكم الدولة والمحاكم الاتحادية. إلا أنه قد تم منح كافة الطلبات الخاصة بتلك السنة. وقد كانت الغالبية العظمى من أوامر التصنت تتعلق بقضايا مُخدرات (1.792 من أصل 2.208 أي بنسبة 81 %)، وكانت أعلى نسبة تالية تتعلق بجرائم القتل وقضايا الاعتداء (132 من أصل 2.208 أي بنسبة 6 %)

⚠ تعرف على أدواتهم

كيف يمكنني معرفة ما إذا كان هاتفي مراقبًا؟

على الأرجح، لن تتمكن من معرفة ما إذا كان هاتفكَ مُراقبًا. إن المراقبة الحكومية قد خطت خطوات ناجحة منذ ذلك الوقت الذي كانت فيه النقرات والصفارات والطنين وغيرها من الأصوات قد تُحذركَ بوجود تصنت. يُفترض عمومًا أن تقوم الحكومة بإخباركَ في غضون 90 يوما بعد انتهاء المراقبة، ولكن من الممكن أن يتم إرجاء الإنذار في حالة الجرائم ذات السهولة النسبية.

ما هو التصنت المُتنقل؟

عادة ما يتم تطبيق عمليات التصنت على هاتف مُحدد في موقع مُحدد وذلك بعد الحصول على ترخيص بأمر من المحكمة. إلا أن التصنت المُتنقل هو التصنت على أي هاتف في أي موقع تعتقد هيئات تنفيذ القانون بأن الهدف قد يقوم بإجراء مُكالمات هاتفية منه. تم السماح للحكومة باستخدام التصنت المُتنقل منذ عام 1998. تحتاج الحكومة إلى تلبية نفس المقاييس المتبعة في عملية التصنت العادية على عمليات التصنت المُتنقل، – ويكون السبب المُرجح هو أن الجريمة قد ارتُكبت أو على وشك أن تُرتكب.

ماذا عن أجهزة التصنت ؟

جهاز التصنت هو جهاز إلكتروني مُصغر يمكنه الاستماع إلى المحادثة وبثها و/أو تسجيلها. من خلال وضع جهاز تصنت في مكتبك أو منزلك، يُمكن لهيئات تنفيذ القانون التصنت على كل ما يُقال داخل نطاق الجهاز. الشروط والمُتطلبات التي تُنظم استخدام أجهزة التصنت هيّ عادةً نفس شروط استخدام عمليات التصنت العادية. استخدام أجهزة التصنت يحتوي على بعض الصعوبات والتي قد تواجه وكلاء تنفيذ القانون ومن هذه الصعوبات: يتعين عليهم تثبيت الجهاز في موقع الهدف؛ هذه الأجهزة عرضة للقصور في الأداء؛ هناك خطر اكتشاف هذه الأجهزة؛ تكون عديمة الجدوى في حالة التشويش الكهربي. بسبب تلك الصعوبات، يتم استخدام أجهزة التصنت بنسبة أقل من عمليات التصنت على الهاتف.

جهاز تسجيل الأرقام وأجهزة "الاعتراض والتعقب"

جهاز تسجيل الأرقام يقوم بتسجيل الأرقام الصادرة من خط الهاتف وتخزينها على الجهاز المُرفق. أجهزة "الاعتراض والتعقب" تقوم بتسجيل أرقام هواتف المكالمات الواردة.

إذا كانت هيئات تنفيذ القانون ترغب في تثبيت واستخدام أي جهاز، فمن الضروري الحصول على أمر من المحكمة؛ إلا أنه من السهل للغاية الحصول على مثل هذه الأوامر. الحكومة بحاجة إلى الاعتقاد بأن المعلومات التي من المُرجح الحصول عليها وثيقة الصلة بالتحقيقات الجنائية الجارية فحسب. عادة ما يقوم القضاة وهيئات تنفيذ القانون بإلقاء نظرة شمولية عن ما قد يكون وثيق الصلة بالتحقيق. هناك العديد من الدول التي تسمح باستخدام مثل هذه المراقبة وفقًا لمعايير أكثر تساهلاً. كما يُمكن للنائب العام الأمريكي أيضًا إجازة استخدام هذه الأجهزة لمدة تصل إلى سبعة أيام دون الحصول على أمر من القاضي وذلك في بعض حالات "الطوارئ"

⚠ تعرف على أدواتهم

جهاز تسجيل الأرقام وأجهزة "الاعتراض والتعقب" (تـــابع ...)

عمل قانون المواطنة على توسيع نطاق الاستخدام المسموح به لكل من جهاز تسجيل الأرقام وأجهزة "الاعتراض والتعقب" على حد سواء. بعض الاستخدامات الموسعة لجهاز تسجيل الأرقام وأجهزة "الاعتراض والتعقب" تشتمل على: تتبعُ الموقع الجغرافي لمستخدمي الهاتف الخلوي؛ تسجيل عناوين مواقع الويب التي تزورها، وعناوين بروتوكول الانترنت التي يتصل بها حسابكَ؛ أو عناوين بروتوكول الانترنت للأجهزة التي يصل بها جهازكَ شبكيًا. عنوان بروتوكول الإنترنت هو رقم فريد من نوعه يتم تخصيصه لكل حاسب أو جهاز يرتبط بشبكة ما.

⚠ تعرف على أدواتهم

ماذا عن برنامج التصنت على الاتصالات الهاتفية بدون مذكرة التابع إلى محكمة مراقبة المخابرات الأجنبية ووكالة الأمن القومي؟

يُمكن للحكومة التصنت على هواتف المواطنين وغير المواطنين إذا كان هناك سبب مرجح للاعتقاد بأن الهدف هو عضو في جماعة إرهابية أجنبية أو وكيل لقوة أجنبية. من أجل التصنت على المكالمات الهاتفية للمواطنين والمقيمين بصفة قانونية، يتعين على الحكومة أيضًا الإفصاح عن السبب المرجح بأن الهدف يُشارك في أنشطة "ربما" تنطوي على مخالفة جنائية. وبالنسبة لهذا النوع من المراقبة، يتعين على الحكومة الحصول على إذن تفتيش من محكمة مراقبة الاستخبارات الخارجية، وهي محكمة سرية والتي تقوم بعقد جلسات اجتماع مُغلقة أمام الجمهور. عبر وكالة الأمن القومي، تقوم الحكومة بمُطالبة السلطات المختصة برصد أية اتصالات هاتفية أو إلكترونية بدون مذكرة قضائية إذا كانت تعتقد أن طرفًا واحدًا فحسب يقيم خارج الولايات المتحدة – وذلكَ حتى إذا كان الطرف الآخر مُقيمًا داخل الولايات المتحدة في حين أن وكالة الأمن القومي تكون بمثابة المخول الوحيد لرصد الاتصالات لأغراض الحصول على معلومات استخباراتية خارجية، ويكون النطاق الكامل للبرنامج غير معروف.

ما هي التهديدات الأمنية التي تمثلها الهواتف الخلوية والهواتف الذكية وأجهزة المُساعد الشخصي الرقمي؟

مُلائمة وسهولة الاتصال عبر الهاتف الخلوي تُسفر عن خصوصية هامة ومخاطر أمنية. يجب أن تكون على دراية وحذر بالمخاطر الكامنة في استخدام هذه الأجهزة والترجيح بين مزايا الملاءمة والخطر الأمني قبل استعمال الهاتف الخلوي.

نفس القواعد القانونية التي تنطبق على الهواتف الأرضية الثابتة تنطبق على زرع أجهزة تصنت أو جهاز تسجيل أرقام أو أجهزة الاعتراض والتعقب" في أي هاتف. إلا أنه من الهام مُلاحظة أن أي شخص يمتلك بضعة مئات من الدولارات تكفي لشراء المعدات سيكون بمقدوره اعتراض إشارات هاتفكَ الخلوي. ولا يتعين عليكَ مُطلقًا افتراض أن كافة الوكلاء يمتثلون للقانون دومًا. يُمكن للأفراد والشركات أيضًا اعتراض إشارات هاتفكَ الخلوي بكل سهولة في ظل تضاءل خطر الإيقاع بهم. تتمتع الحكومة بالقدرة على تحويل الهاتف الخلوي إلى جهاز استماع أو "جاهز تصنت مُتنقل". هذا الأمر يُمكن الحكومة من الاستماع إلى أية مُحادثات يتم إجراؤها بالقرب من الهاتف الخلوي. الحكومة لا تحتاج إلى الوصول إلى الهاتف الخلوي ذاته من أجل "زرع" جهاز التصنت، ولكن يُمكنها فعل ذلكَ ببساطة من خلال شركة هاتفكَ الخلوي. أجهزة التصنت المُتنقلة تُمكن الحكومة من الاستماع إلى المُحادثات التي يتم إجراؤها بالقرب من هاتفك الخلوي حتى عند إيقاف تشغيله. إلا أن إزالة البطارية من الهاتف الخلوي سيقوم بتعطيل أجهزة التصنت المُتنقلة.

يُمكن استخدام هاتفكَ الخلوي في تتبع موقعكَ. يكون هاتفكَ الخلوي على اتصال بواحد أو أكثر من أبراج الشبكات الخلوية في منطقتكَ، وذلكَ حينما يكون هاتفكَ الخلوي يعمل ويتلقى إشارة. يمكن للحكومة مراقبة هذه الاتصالات لتحديد موقعك في المدن والمناطق الأخرى ذات الكثافة العالية من أبراج الشبكات الخلوية، يمكن تعقب موقعك بدقة أكبر، وأحيانًا يتم تحديد الموقع على بعد بضعة ياردات. لا يوجد أي معيار قانوني موحد لهذا النوع من تتبع الهاتف الخلوي في الوقت الراهن. بعض المحاكم تطلب من الوكلاء تلبية ذات المتطلبات القانونية اللازمة للحصول على جهاز تسجيل الأرقام أو جهاز الاعتراض والتعقب. بينما هناك محاكم أخرى تتطلب من الوكلاء الحصول على مُذكرة مُدعمة بسبب مُرجح. قد تتمكن الحكومة من استعراض سجلات هاتفكَ السابقة لتحديد موقعكَ آنذاك إذا كان هاتفكَ الخلوي قيد التشغيل حينها.

بعض المحاكم تمنح مُذكرة لهيئات تنفيذ القانون تُجيز لهم تفتيش سجل المكالمات وقائمة الاتصالات المخزنة على هاتفكَ وذلكَ فور اعتقالكَ. كما أن هناك بعض المحاكم تُجيز لهيئات تنفيذ القانون تفتيش الرسائل النصية والصور ورسائل البريد الالكتروني وأية سجلات أخرى موجودة في هاتفك فور إيقافك قانونيًا. وبعض المحاكم تُجيز لهيئات تنفيذ القانون تفتيش سجلات المكالمات دون مُذكرة، مُدعيةً أن تفتيش سجلات المكالمات سيُسفر عن نفس المعلومات التي يمكن الحصول عليها من جهاز تسجيل الأرقام، إلا أنها تقتضي وجود مُذكرة للتفتيش في الرسائل النصية أو رسائل البريد الإلكتروني. لا تزال المحاكم تعمل على تطوير هذا النطاق من القانون؛ ونتيجة لذلكَ، تختلف القوانين واللوائح من ولاية قضائية إلى أخرى. تفعيل حماية هاتفكَ الخلوي باستخدام كلمة السر تمنحكَ مستوى مُعين من الحماية ضد المخاطر الأمنية الكامنة في استخدام الهاتف الخلوي.

هل يمكن للحكومة مراقبة رسائلي النصية؟

الرسائل النصية هي طريقة اتصال غير آمنة إلى حد كبير. حيث يُمكن اعتراض الرسائل النصية بسهولةً من قبل أي شخص يستخدم المعدات الصحيحة، مثلماَ قد يحد في المحادثات الهاتفية. لم يتحد الكونجرس أو المحاكم بوضوح عمّا إذا كان من الضروري وجود سبب مُحتمل أو مُذكرة لاعتراض الرسائل النصية، لذا، ربما تقوم هيئات تنفيذ القانون بمحاولة اعتراض الرسائل النصية باستخدام أوامر تسجيل الأرقام أو جهاز الاعتراض والتعقب والتي يسهل الحصول عليها نسبيًا. وأخيرًا، لأن الرسائل النصية لا تُعتبر "اتصالات سلكية"، فمن ثم لا تتمتع بالحماية المنصوص عليها في قاعدة استثناءات قانون التصنت. لذلك حتى إذا كانت الحكومة قد اعترضت رسائلكَ النصية وقراءتها بشكل غير قانوني، إلا أنه يحق لها الاستمرار في استخدام هذه الرسائل ضدك في محاكمة جنائية.

اتصالات الإنترنت

هل يمكن للحكومة قراءة رسائل بريدي الإلكتروني؟

يمكن لهيئات تنفيذ القانون الوصول بسهولة إلى الكثير من اتصالاتكَ الإلكترونية والمعلومات التي تتضمنها. الحكومة بحاجة إلى الاعتقاد بأن المعلومات التي من المرجح الحصول عليها وثيقة الصلة بالتحقيقات الجنائية الجارية فحسب، وذلكَ للحصول على مذكرة تُجيز الوصول إلى اتصالاتكَ الإلكترونية. بموجب هذه المذكرة، يمكن للحكومة الحصول على "معلومات المشترك الأساسية" الخاصة بكَ والتي تتضمن الاسم والعنوان الفعلي المرتبط بالحساب؛ مدة ونوع الخدمة المستخدمة؛ السجلات؛ عنوان بروتوكول الإنترنت الخاص بحاسبكَ. الحكومة بحاجة إلى أمر "د" (انظر "تعرف على أدواتهم: أمر د") للحصول على "سجلات خارج المحتوى" والتي تتضمن أية تسجيلات أو سجلات تُظهر عناوين البريد الإلكتروني قمت بإرسال أو استلام رسائل إلكترونية منه أو إليه؛ أوقات وتواريخ إرسال أو استلام رسائل البريد الإلكتروني؛ ومساحة كل بريد إلكتروني.

يتم تطبيق طريقة حماية مُختلفة بالاستناد إلى كيف كانت رسائل البريد الإلكتروني الأخيرة وما إذا كنت قرأتها من عدمه، وذلك فيما يتعلق بالبريد الإلكتروني المخزن من قبل طرف ثالث، مثل خدمة البريد الإلكتروني على الويب أو موفر خدمة الإنترنت. قانون الاتصالات المخزنة يُلزم هيئات تنفيذ القانون بالحصول على مذكرة تفتيش محتوى رسائل البريد الإلكتروني (أسطر وفحوى الموضوع) والتي لم يتم فتحها وهيّ قيد التخزين لمدة أقل من 180 يوم. يُمكن للحكومة الحصول على أمرٍ "د" أو إصدار مُذكرة بتفتيش محتوى الرسائل، وذلك بالنسبة للرسائل التي يتم فتحها لمدة تزيد عن 180 يوم وأيضًا عن رسائل البريد الإلكتروني المفتوحة والمخزنة من قبل أي طرف ثالث. قد تقوم الحكومة أيضًا بتفضيل الحصول على مذكرة تفتيش لرسائل البريد الإلكتروني التي تتجاوز 180 يوم أو رسائل البريد الإلكتروني التي تم فتحها.

في الولايات التي تقع ضمن اختصاص محكمة الاستئناف الدائرة التاسعة وهيّ ألاسكا وأريزونا وكاليفورنيا وهاواي وايداهو ومونتانا ونيفادا وأوريغون وواشنطن، اختلفت المحاكم مع الحكومة من حيث تفسير إمكانية الحكومة بموجب أمر "د" أن تحصل على رسائل البريد الإلكتروني المفتوحة والتي تم تخزينها لمدة أقل من 180 يوم. حيث قضت هذه المحاكم بأنه يتعين على الحكومة الحصول على مذكرة تفتيش لفتح أية رسائل بريد إلكتروني مُخزنة لمدة أقل من 180 يوم.

من المفترض أن تقوم الحكومة بإرسال إشعار مُسبق إلى الشخص المشترك قبل استخدام أوامر "د" أو مذكرة استدعاء للحصول على محتوى البريد الإلكتروني. من الناحية النظرية هذا الأمر من شأنه أن يسمح للمشترك اتخاذ التدابير للتصدي لمذكرة الاستدعاء قبل أن يقوم الطرف الثالث بالإذعان لها. غير أن هناك فقرة أخرى من فقرات قانون الاتصالات المخزنة تُجيز لهيئات تنفيذ القانون إرجاء إشعار الأمر "د" أو مذكرة الاستدعاء لفترة طويلة من الزمن. ويبدو أن المحكمة دومًا تقوم بإرجاء الإشعار بانتظام. يُمكن لهيئات تنفيذ القانون أيضًا تجنب إرسال الإخطار لكَ من خلال اتخاذ الخطوات الإضافية اللازمة للحصول على أمر تفتيش.

هل يمكن للحكومة قراءة رسائل بريدي الإلكتروني؟ (تـابع ...)

أكبر مزودي خدمات الإنترنت يتلقون أكثر من 1000مذكرة استدعاء كل شهر وذلك بغرض الحصول على معلومات عن مُستخدميهم. مُعظم هذه المذكرات تطلب معرفة أسماء المستخدمين وعناوينهم وعناوين مقدمي خدمات الإنترنت وتسجيلات بأوقات خروج ودخول الهدف من وإلى شبكة الإنترنت .

هناك العديد من تقارير برامج هيئات تنفيذ القانون تهدف إلى رصد كميات كبيرة من حركة السير على الإنترنت بما في ذلك رسائل البريد الإلكتروني وأنشطة الويب. لم يُعرف بعد مدى هذه البرامج، أو استخدامها المرخص ومدى قبول أي من المعلومات تم الحصول عليها من خلالهم في المحكمة.

هل يمكن للحكومة معرفة مواقع الإنترنت التي قمت بزيارتها؟

تحتاج هيئات التنفيذ القانوني إلى تصريح للوصول إلى سجلات زياراتك الفعلية للمواقع الإلكترونية. ووفقاً للتقارير تستطيع الحكومة تحديد رابط تحديد المصدر الموحد "URL" مثل:
http://ccrjustice.org لكافة المواقع التي قمت بزيارتها؛ لكن تكون الحكومة بحاجة إلى إصدار تصريحاً بالحصول على الصفحات التي قمت بزيارتها في هذا الموقع تحديداً ، فمثلاً:
http://ccrjustice.org/ifanagentknocks

الأوامـــــر "د"

يعد الأمر "د" رقم 2307 من وسائل تنفيذ القانون شائعة الاستخدام والذي يشار إليه "الأمر د". وقد أطلق على الأمر "د" هذا الاسم من القسم الفرعي الذي نص عليه في قانون الاتصالات المخزنة. تستخدم الحكومة الأمر "د" للحصول على السجلات الإلكترونية التي يتم تخزينها لدى أطراف خارجية – وعادة ما يكون الحصول على أمر "د" أصعب من الحصول على مذكرة استدعاء لكنه أسهل من الحصول على إذن تفتيش. وحتى تتمكن الحكومة من الحصول على أمر "د" يجب أن تقوم بتقديم الحقائق إلى القاضي والتي تدل على توافر الخلفية المعقولة لاعتقادها بأن هذه المعلومات متعلقة بالجريمة التي يجري التحقيق فيها. لذلك فإن الشك الذي يوجب استصدار الأمر "د" أقل من أن يكون سبباً محتملاً، لكنه أعلى من أن يكون نموذجاً "لأي سبب ممكن" يتطلبه الحصول على مذكرة استدعاء.

⚠ تعرف على أدواتهم

هل يتعين علي التزام الحذر من المراقبة الإلكترونية من قبل كيانات غير حكومية؟

إن تجسس الشركات يعد صناعة أكبر بكثير من التجسس من قبل الحكومة. تقوم الشركات بتعيين جواسيس بصفة روتينية، والذين يكون أغلبهم من المخبرين السابقين لدى هيئات لتنفيذ القوانين، وذلك بغرض مراقبة الأنشطة التي قد تهدد اهتماماتها. تضم عمليات التجسس من الشركات عدة تكتيكات من المتبعة في الحكومة، بما في ذلك، البحث في النفايات؛ ومراقبة الهواتف، وتتبع الأنشطة على الإنترنت؛ وقد تستخدم المخترقين. عادة لا يهتم جواسيس الشركات بالقيود المفروضة على عمليات التجسس.

خطابات الأمن القومي

خطابات الأمن القومي هي أداه يستخدمها مكتب المباحث الفيدرالية في الطلب السري لمعلومات عن الأفراد من طرف ثالث، مثل شركة الهواتف، ومزودي خدمات الإنترنت، ووكالات أرصدة المستهلكين أو المؤسسات المالية. لا تحتاج خطابات الأمن القومي إلى تواجد سبب مرجح أو رؤية شاملة – يكفي أن تكون المباحث الفيدرالية مقتنعة لأن المعلومات التي تسعى للحصول عليها متعلقة بأعمال إرهابية أو تجسسية – وتضم قوانين خطابات الأمن القومي قاعدة حماية تمنع من حصل عليها من الإفصاح عن حصوله عليها إلا لمحاميه. ومع ذلك، فقد رأت المحكمة مؤخراً خلال التداول أن قاعدة الحماية تلك غير دستورية، ويبقى تطبيقها مستقبلاً غير واضح.

قد أكدت دراسات حكومية أن المباحث الفيدرالية تصدر عشرات الآلاف من خطابات الأمن القومي كل عام، وتقوم بخرق حتى القيود الثانوية من خلال سلطتها لإصدار هذه الخطابات. يتم تداول محتوى خطابات الأمن القومي فيما بين أجهزة الاستخبارات الأمريكية، والمنظمات الحكومية الأخرى وحتى مع الحكومات الأجنبية.

في حالة تسلمك أنت أو المنظمة التي تعمل بها أحد خطابات الأمن القومي، يجب أن تتصل فوراً بالمحامي.

⚠ تعرف على أدواتهم

الأمـــن الإلكـــتروني

يمثل الأمن الإلكتروني موضوعاً شائكاً ومعقدًا. يقدم هذا الفصل بعضاً من أهم النصائح الرئيسية فيما يتعلق بالأمن الإلكتروني. وستجد معلومات أكثر تعمقاً بهذا الشأن في قسم المصادر الإضافية الملحق بهذا الدليل.

ببساطة، لا تعتبر الاتصالات الإلكترونية الأكثر أمناً اتصالات إلكترونية على الإطلاق. تتطلب عادات الأمن الإلكتروني الفعالة الحفاظ الدائم على التوازن بين الملائمة والمخاطر المصاحبة للتواصل إلكترونياً. كما هو الحال في أي ممارسة، يجب أن تقارن بين المخاطر والمكاسب قبل اختيار وسائل الأمن الإلكتروني التي تستخدمها.

تشفـير البيـانات

التشفير هو طريقة لتحويل المعلومات إلى رموز معقدة. عند استخدامها بالطريقة السليمة، فإن التشفير يحول دون اطلاع أي شخص لا يمتلك الصلاحية اللازمة على بياناتك. تعتبر تقنيات التشفير الحديثة صعبة جداً حيث تجعل من المستحيل على الحكومة أن تقوم بحل شفرة الرسائل دون استخدام الصلاحيات. فالتشفير هو الحماية الأقوى لتمنع الحكومة من الحصول على بيانات الإلكترونية.

تتوافر برامج التشفير بشكل شاسع والتي تمكنك من تشفير كافة البيانات المسجلة على القرص الصلب الخاص بك. فكلمات المرور البسيطة للولوج إلى الحاسب ليست كافية لحماية البيانات على القرص الصلب. تستطيع الحكومة أن تصادر قرصك الصلب وتقوم بنسخ محتوياته بكل سهولة وتصل إلى البيانات دون الحاجة إلى الولوج إلى حسابك. لكن بتشفير القرص الصلب، سيتم ترميز بياناتك ولن تستطيع الحكومة الوصول إليها بدون كلمة سر التشفير.

كما تسمح لك برامج التشفير بتشفير ملفات أو مجلدات بعينها. بينما يكون من السهل تدبر ذلك، لكن قد يعرض التشفير المنفصل هذه الملفات لأخطار أكبر. فمن الأفضل أن تحتفظ بقرص صلب مستقل ومشفر بالكامل لملفاتك الحساسة.

تعرف على أدواتك

الأمـــن الإلكـــتروني

تشفير البريد الإلكتروني

إن استخدام التشفير قد يكون أكثر أهمية للبريد الإلكتروني. لقد أوضحنا سابقاً كيف يمكن أن تستخدم الحكومة الأوامر "د" أو مذكرات الاستدعاء للحصول على صلاحية الوصول إلى بريدك الإلكتروني أو أي من الأدوات الأخرى التي تعترض سبيلهم خلال الانتقال. وبما أن البريد الإلكتروني يحفظ على حاسب طرف آخر فلا يمكنك التحكم في من يطلع عليه ويقرأه. كما هو الحال مع تشفير البيانات، هناك أداة واحدة لحماية اتصالاتك الإلكترونية ألا وهي تشفير البريد الإلكتروني. في سبيل الاستخدام الفعال لتشفير البريد الإلكتروني، يجب تستخدم أنتَ والشخص الذي تتواصل معه برامج التشفير.

يضمن تشفير البريد الإلكتروني أنه لن يتمكن أي فرد من الاطلاع على الرسالة سوى الشخص المعني والذي تم إرسالها إليه. يعمل نظام تشفير البريد الإلكتروني الحديث باستخدام "مفاتيح عامة". تعمل المفاتيح العامة على توفير الإرشادات والرموز التي تساعد على فك شفرة البريد الإلكتروني وكيفية فعل ذلك. يختلف الكود الخاص بالرسالة غير المفهومة – "المفاتيح الخاصة" – عن المفاتيح العامة، وأنت وحدك الذي يملك صلاحية الوصل إلى المفاتيح الخاصة.

لو تقاطع بريدك الإلكتروني مع مذكرة الاستدعاء، أو أمر المحكمة أو غيرها، فلن يمكن فك شفرة هذه الرسالة وفهمها دون مفاتيحك الخاصة.

في الحين أن التفاصيل الفنية لتشفير البريد الإلكتروني أكبر من أن يتم ذكرها في هذا الدليل، فيمكن تعريف التشفير بطريقة بسيطة كأنه باب مفتوح يمكن لأي فرد إغلاقه لكن لا يمكن فتحه إلا بمعرفة شخص واحد يملك مفتاحاً خاصاً.
إن تشفير البريد الإلكتروني أسهل بكثير في يومنا هذا عما كان عليه في الماضي.

برنامج التشفير (GnuPG) هو برنامج مجاني يمكن أن يتم إدراجه في معظم برامج البريد الإلكتروني. على سبيل المثال، إن خدمة البريد الإلكتروني المقدم من موزيلا الذي يطلق عليه "Thunderbird" تحتوي على ملحق يعرف أيضاً باسم "Enigmail" والذي يتوافق مع التشفير باستخدام (GnuPG) والذي قد جعل من التشفير أمراً أسهل بكثير.

تعرف على أدواتك

الأمـــن الإلكـــتروني

كلمات المرور

لتأخذ كلمات المرور على محمل الجد. لا تستخدم الكلمات أو الكلمات التي تحتوي على أرقام في أخرها أو وسطها. حيث أنه يمكن كسر كلمات المرور هذه بسهولة بعد عدة محاولات. استخدم سلسلة من الأحرف والتي قد تعني شيئاً بالنسبة لك فحسب. لا تستخدم نفس كلمة المرور لأكثر من مرة لحسابات مختلفة تحتوي على بيانات شخصية. حاول الاحتفاظ بكلمات المرور في ذاكرتك. يمكن أن تُكتشف كلمات السر المكتوبة. التزم بتغيير كلمة المرور كل عدة أشهر. لو اضطررت لكتابة كلمة المرور، فحاول كتابتها برموز لا يفهمها غيرك. لو قررت أن تكتب كلمة المرور الخاصة بك فلا تتركها أبداً بالقرب أو بجوار الحاسب الآلي؛ ويجب أن تكف عن الاحتفاظ بهم في محفظة جيبك.

ولتحاول استخدام برنامج "Password safe" فمثل هذه البرمجيات تساعدك على الاحتفاظ بكلمات المرور الخاصة بك في ملف واحد مشفر على حاسبك الشخصي، لذلك لن يكون عليك تذكر سوى كلمة مرور واحدة لتصل إلى كافة كلمات المرور الأخرى. لا تكتب أبداً كلمة المرور الرئيسية، حيث إنها هي كلمة المرور التي تحمي باقي الكلمات الأخرى.

تصفح الإنترنت

كن حريصاً في التعامل مع البيانات أثناء تصفحك للإنترنت، فقد يحتفظ المتصفح ببياناتك وأنشطتك على الإنترنت والبيانات التي قد تتوافر لدى المواقع الأخرى عنك.

بشكل ثابت، تحافظ متصفحات الانترنت على قدر كبير من المعلومات الخاصة بما في ذلك ودون الاقتصار على : مواقع الويب التي تزورها، كلمات مرور تلك المواقع، وحتى صور من صفحات الويب التي تقوم بزيارتها إن العميل الذي يمكنه حيازة المشغل الصلب خاصتك يمكن أن يعلم الكثير عن نشاطك على الانترنت من خلال تلك الملفات. قم بمسح هذه المعلومات بشكل منتظم. قم بضبط متصفحك لمسح تاريخ تصفح الانترنت، الملفات المخبأة، كوكيز، تاريخ التحميل، النماذج المحفوظة، وكلمات المرور المحفوظة بانتظام. ربما تود القيام بهذا يومياً أو وقتما تغلق متصفحك. أينما يكون متاحًا، استخدم التشفير المثبت على موقع الويب عند التصفح لتجنب اعتراض طرف آخر للمعلومات المرسلة. تبدأ المواقع ذات التشفير المثبت بـ https بدلاً من http.

أهتم باستخدام أدوات انترنت مجهولة مثل Tor. وهو برنامج تشفير وإخفاء يعمل على نقل بياناتك فقط من خلال برنامج Tor الخاص بالعملاء الآخرين، تشفير بياناتك طوال المسار واستبعاد المعلومات الخاصة بمكان بدء البيانات. ويعرف كل موجه Tor فقط عنوان آخر موجه مر به، مما يجعل من الصعوبة الشديدة تتبع أي اتصال إلى مصدره الأصلي. هناك بعض العيوب لاستخدام برنامج Tor وهي السرعات المنخفضة التي يتم عندها تحميل صفحات الويب، والعديد من الوظائف غير المؤمنة مثل أن الفلاش لا يعمل مع برنامج Tor.

تعرف على أدواتك

الأمـــن الإلكـــتروني

تعرف على موردي خدمة الانترنت إليك

قم بقراءة شروط الخدمة وسياسات الخصوصية الخاصة بأي خدمة إلكترونية تفكر في الاشتراك بها. بعض ISPs ، بما في ذلك الكثير من تلك المجهزة لتلبية احتياجات النشطاء السياسيين، توفر نظم حماية أقوى للخصوصية وتزعم أنها أكثر مقاومة للتجسس الحكومي.

استخدام البرامج المضادة لبرمجيات التجسس Anti-Spyware

قم بشراء برنامج جيد مضاد للتجسس و/أو الفيروس ، وأعمل على تحديثه بشكل منتظم. تستطيع برمجيات التجسس خرق كافة الإجراءات الأمنية الإلكترونية لديك، الدخول على كل موقع قمت بزيارته، وكل كبسة زر على جهازك. تزعم شركات البرامج المضادة للتجسس الكبرى أنها تتعامل مع برمجيات التجسس الحكومي مثلما تتعامل مع أي برمجيات تجسس أخرى.

استعادة ومسح البيانات

لا يمكن للحكومة الحصول على ما ليس له وجود. قم بوضع سياسة لاستعادة البيانات تقوم فيها بعرض ومسح الملفات القديمة بشكل ثابت. لا تقم بمسح المستندات عشوائياً – أختر وقت محدد والتزام به. يمكنك إنشاء جدول مختلف لمختلف أنواع البيانات، على سبيل المثال، قم بمسح ملفات الحاسب الآلي كل شهرين، قم بسمح رسائل البريد الإلكتروني كل أسبوعين، وأمسح مدخلات متصفح الويب كل يومين. مهما كانت سياستك، التزم بها. في النهاية، هل تحتاج فعلاً إلى رسائل البريد الإلكتروني خلال الثلاثة أعوام الماضية؟ لا تقم بمسح أي شيء تم استدعاؤه – إذا قمت بذلك، تكون قد قمت بارتكاب المخاطرة الجسمية وهي تهمة عرقلة سير العدالة. احتفظ بسجل كتابي بسياسة استعادة بياناتك لحماية نفسك ومنظمتك من اتهامات تدمير البراهين.

تعرف على أدواتك

هيئات المحلفين الكبرى ومقاومة هيئة المحلفين

هيئة المحلفين الكبرى هي عبارة عن هيئة من المواطنين الذين تم جمعهم معاً للتحقيق في الجرائم وإصدار الأحكام. في مفهومها الأصلي، كانت هيئة المحلفين تهدف إلى أن تكون ديمقراطية بشكل جذري. في إنجلترا، عملت كحاجز بين المواطنين وعاهل المملكة ونواب العموم. في بداية ظهور أمريكا، كان أي مواطن يستطيع اتهام هيئة المحلفين باقتراف الخطأ، وكانت هيئة المحلفين الكبرى توجه الاتهام على أساس تصويت الأغلبية.

في العصر الحديث، أصبحت هيئة المحلفين شديدة الاختلاف. اليوم، يتم عرض كافة القضايا على هيئة المحلفين الكبرى من قبل النائب العام. ويقوم النائب العام باختيار الشهود وطرح الأسئلة. لا يُسمح للشهود بحضور محاميهم. لا يوجد قاض. يقوم النائب العام بعرض الاتهامات وقراءتها على هيئة المحلفين. لا يتطلب الأمر أن يكون أعضاء هيئة المحلفين على علم بالقانون ذات الصلة. وعلى خلاف هيئات المحلفين الكبرى الأخرى، لا يخضع أعضاء هيئة المحلفين لاختبار التحيز.

ما هي هيئات المحلفين الكبرى وما هي التهديدات التي تشكلها على النشطاء؟

نظراً لأن النائب العام يقوم بشكل منفرد بتنظيم الإجراءات، فلا عجب أن هيئات المحلفين الكبرى دوماً ما تكون مصدقة تلقائياً للنيابة. أشار قاض سابق شهير في نيويورك قائلاً : "أي نائب عام له الرغبة في الاتهام، يمكنه حتى اتهام سندويتش اللحم". في الحالات النادرة التي لا تقوم هيئة المحلفين فيها بالاتهام، يمكن للنائب العام ببساطة تشكيل هيئة محلفين أخرى ويطلب الاتهام أمام هيئة محلفين جديدة.

في القضايا السياسية، كان يتم استخدام هيئات المحلفين الكبرى لتنفيذ المطاردات ضد النشطاء. يقوم نواب العموم بإحضار شهود نشطاء ويحاولون جعلهم يوشون بغيرهم من النشطاء مع التهديد بالسجن، في حالة رفضهم التعاون مع هيئة المحلفين. من الصعب فهم كيفية عمل هيئة المحلفين، ما هي حقوقك، ما هي الحقوق التي لا يمكنك ممارستها، وكيفية مقاومة هيئة المحلفين.

ما هي هيئات المحلفين الكبرى وما هي التهديدات التي تشكلها على النشطاء؟ (تـابع ...)

هناك العديد من الحقوق التي نسلم بعدم وجودها لشهود هيئة المحلفين. لا يحق لشهود هيئة المحلفين أن يقوم بتمثيلهم وكيل ولا يحق لهم طلب محاكمة المحلفين في حالة تهديدهم بالسجن. يحتفظ شهود هيئة المحلفين بالحق ضد التجريم الذاتي ولكن قد يتم إجبارهم على أن يوشوا بأنفسهم وغيرهم مقابل الحصانة من المقاضاة والعقاب. تحمي الحصانة الشهود فقط – يمكن مقاضاة غيرهم.

ماذا افعل إذا ظهر شخص ما ومعه استدعاء هيئة المحلفين؟

يقوم مسؤولو تنفيذ القانون بتسليم استدعاءات هيئة المحلفين، عادة ما يكونوا ضباط شرطة أو مارشال فيدرالي. يجب أن يتم تسليم استدعاء هيئة المحلفين شخصياً إليك، مما يعني يجب تسلمه يداً بيد إليك. إذا رفضت استلامه، يجب أن يوضع بالقرب منك.

لا يمنح استدعاء هيئة المحلفين العميل الحق في تفتيش المنزل، المكتب، السيارة، أو أي مكان آخر، كما لا يتطلب منك تقديم أية مستندات أو قول أي شيء في هذا الوقت. يتطلب استدعاء هيئة المحلفين منك فقط القيام بشيء ما في التاريخ المستقبلي المحدد في الاستدعاء.
إذا جاءك عميل وحاول تسليمك أمر إحضار أمام المحكمة، تسلمه منه ولا تفعل أي شيء آخر.
فلا تجب على أي أسئلة ولا توافق على قيامه بالتفتيش ولا تدعوه إلى منزلك لأي سبب كان.

أوامر الإحضار أمام هيئة المحلفين الكبرى

تحصل هيئات المحلفين الكبرى على معلومات من الأشخاص بواسطة إصدار أوامر إحضار. أمر إحضار أمام هيئة المحلفين الكبرى هو بمثابة أمر للإدلاء بالشهادة أمام هيئة محلفين كبرى أو تزويدها بمعلومات معينة. تقوم هيئات المحلفين الكبرى بإصدار أنواع مختلفة من أوامر الإحضار للشهادة وتقديم المعلومات. يعد أمر "subpoena ad testificandum"، أو الاستدعاء للشهادة، عبارة عن أمر مثول أمام المحكمة يأمر الشاهد بالحضور والإدلاء بشهادته. بينما يعني بالأمر "subpoena duces tecum"، والذي يعني باللغة اللاتينية "أحضرها معك"، فهو أمر إحضار لأمر الشاهد بتقديم مستندات معينة إلى هيئة المحلفين. تستخدم هيئات المحلفين الكبرى تلك الأوامر للحصول على بصمات الأصابع وعينات من خط اليد. وعادة ما تصدر هيئات المحلفين الكبرى الأمرين إلى نفس الشاهد ليتمكنوا من الحصول على المستندات والشهادة.

⚠ تعرف على أدواتهم

ما هي الخيارات المتاحة أمامي في حالة ما تلقيت مذكرة إحضار أمام هيئة محلفين كبرى؟

يقوم مسؤولو تنفيذ القانون بتسليم استدعاءات هيئة المحلفين، عادة ما يكونوا ضباط شرطة أو مارشال فيدرالي. يجب أن يتم تسليم استدعاء هيئة المحلفين شخصياً إليك، مما يعني يجب تسلمه يداً بيد إليك. إذا رفضت استلامه، يجب أن يوضع بالقرب منك.

لا يمنح استدعاء هيئة المحلفين العميل الحق في تفتيش المنزل، المكتب، السيارة، أو أي مكان آخر، كما لا يتطلب منك تقديم أية مستندات أو قول أي شيء في هذا الوقت. يتطلب استدعاء هيئة المحلفين منك فقط القيام بشيء ما في التاريخ المستقبلي المحدد في الاستدعاء.
إذا جاءك عميل وحاول تسليمك أمر إحضار أمام المحكمة، تسلمه منه ولا تفعل أي شيء آخر.

فلا تجب على أي أسئلة ولا توافق على قيامه بالتفتيش ولا تدعوه إلى منزلك لأي سبب كان. فور تسلمك أمر إحضار صادر عن هيئة محلفين كبرى، يكون متاحاً لك ثلاثة خيارات: 1) يمكنك الامتثال إلى أمر الإحضار، 2) يمكنك اتخاذ الخطوات اللازمة لإسقاط أمر الإحضار، أو 3) يمكنك رفض الامتثال. إذا تسلمت أمر إحضار، يتعين عليك الاتصال بمحامي على الفور ومناقشته في الخيارات الثلاثة المتاحة بالتفصيل.
إن الامتثال لأمر إحضار يعد تصرفاً مباشراً نسبياً. االنسبة إلى أمر "– subpoena ad testi candum"، "الاستدعاء للشهادة، فإنك تحضر في التاريخ والوقت والمكان المحددين في أمر الإحضار وتجيب على أسئلة المدعي العام.
أما بالنسبة إلى أمر "subpoena duces tecum"، أمر إبراز المستندات، فإنك تحضر في التاريخ والوقت والمكان المحددين في أمر الإحضار ومعك المستندات أو الأدلة الأخرى المطلوبة.

ما هي الخيارات المتاحة أمامي في حالة ما تلقيت مذكرة إحضار أمام هيئة محلفين كبرى؟ (تـــابع ...)

إذا امتثلت إلى أمر إحضار، فإنك بذلك تتجنب إمكانية التعرض للعقاب لتجاهلك إياه، ومع ذلك، يمكن للامتثال له أن يعرضك إلى نوع آخر من المشكلات. على سبيل المثال، إذا كنت هدفاً للتحقيق، فإن الامتثال إلى أمر الإحضار قد يزود الحكومة بمعلومات تستخدمها لتوجيه التهم إليك وإدانتك. كما قد تعرض ناشطًا آخر للخطر نتيجة لامتثالك لأمر الإحضار.

إذا تلقيت أمر إحضار، يتعين عليك التحد إلى محامي قبل اتخاذ أي إجراء. إذا كان الدافع وراء أمر الإحضار دافعاً سياسياً، سيكون من الأفضل التحد إلى محامي ينتمي إلى نفس دائرة نشاطك السياسي ويمارس الدفاع الجنائي أمام هيئات المحلفين الكبرى.

قد يقترح بعض محاميي الدفاع الجنائي غير النشطين أن تصبح واشياً. ومع ذلك، من الضروري أن تنتبه إلى أنه كثيراً ما ينتهي الحال بالعديد من الواشين بقضاء سنوات عديدة وراء القضبان مثلهم مثل هؤلاء الذين وشوا بهم. تتم إجراءات هيئات المحلفين الكبرى سراً. حيث عادة لا يعرف مجتمع النشطين حينما يجري تحقيق أمام هيئة محلفين كبرى. ونتيجة لذلك، يعتقد الكثير من النشطاء أنه بالأحرى بهم الإعلان عن تلقيهم أمر إحضار، وهو ما يعد تكتيك فعال يتعين عليك مناقشته مع محاميك إذا ما تلقيت أمر إحضار.

كيف يمكنني إسقاط مذكرة إحضار أمام هيئة محلفين كبرى؟

يمكنك إسقاط أمر إحضار بالمحكمة عن طريق طلب إسقاط أمر إحضار. إن إسقاط أمر إحضار يعني أن تعلن المحكمة كونه ملغى وباطل. لن تصدق المحكمة على طلب إسقاط إلا إذا كان متوافراً دوافع قانونية قوية لتحقيق ذلك؛ مثل خطأ في تحديد الهوية أو عدم الاختصاص القضائي؛ حق امتياز محمي؛ أو عدم شرعية الإجراءات القضائية. حتى إن لم تنجح في إسقاط أمر إحضار، فإن تقديم طلب الإسقاط أمام المحكمة سوف يمنحك بعض الوقت، وهو ما يعد أمراً هاماً ولا سيما إذا كنت تعتزم عدم التعاون مع هيئة المحلفين، حيث إن عدم التعاون قد ينتهي بك في السجن. قد تستمر الإجراءات أمام هيئات المحلفين الكبرى لفترة تصل إلى 18 شهراً ؛ وأياً كان الوقت المستغرق، فإن مقاضاة طلب الإسقاط قد يوفر عليك قضاء المدة بأكملها داخل السجن.
بينما ليس هناك الكثير لتخسره عن طريق تقديم طلب إسقاط أمر "subpoena duces tecum"، فإن أوامر الإحضار التي تتطلب توافر أدلة، طلبات إسقاط "subpoenas ad testifi candum"، التي تتطلب الإدلاء بالشهادة، قد تمثل مشكلة. فلقد حكمت محكمة دائرة فدرالية واحدة على الأقل بأنك تخسر أي اعتراض لم يتم رفعها ضمن الطلب الأصلي بالإسقاط. لذا عليك عدم التنازل عن أي حق اعتراض، وعلى الأخص إنك قد لا تعرف ما هي حقوق اعتراضك حتى يتم سؤالك سؤال معين.
يجب أن يكون المحامي السياسي الجيد قادراً على تقديم النصيحة بشأن ما إذا كان من الأفضل طلب إسقاط أمر إحضار أم لا في ظل ظروفك الخاصة.

ماذا يحدث إذا رفضت الامتثال إلى مذكرة إحضار أمام هيئة محلفين كبرى؟

ثمة طريقتين أساسيتين لفرض الامتثال إلى أمر إحضار أمام هيئة محلفين كبرى: 1) رفض الحضور؛ أو 2) رفض الإجابة على أي من أسئلة المدعي العام. إذا رفضت ببساطة الحضور للإدلاء بشهادتها، فقد تعتبر بذلك في حالة عصيان للمحكمة وقد تقرر الحكومة إلقاء القبض عليك واحتجازك حتى تقوم بالإدلاء بشهادتك أو إلى انتهاء عمل هيئة المحلفين الكبرى. إذا لم تكن شهادتك بالغة الأهمية بالنسبة إلى المدعي العام، فقد يختارون عدم اتخاذ أي إجراء.

ماذا يحدث إذا امتثلت إلى مذكرة إحضار أمام هيئة محلفين كبرى؟

إذا حضرت للإدلاء بشهادتك، لن يسمح لك بحضور محام. ومع ذلك، يمكن حضور محاميك خارج غرفة هيئة المحلفين الكبرى حيث يكون في وسعك استشارته بعد كل سؤال، على الرغم من قيام بعض المحاكم بالحكم بعدم جواز استشارة المحامي إلا بعد كل مجموعة صغيرة من الأسئلة. حيث إنك تحتفظ بحقك في التعديل الخامس ضد التجريم الذاتي، يمكنك رفض الإجابة على أسئلة المدعي العام بقولك "أنا استشهد بامتياز التعديل الخامس ضد التجريم الذاتي" عقب كل سؤال. في هذه المرحلة، قد يقوم المدعي العام ببساطة بصرفك أو السعي إلى منحك الحصانة. تعمل الحصانة على حماية الشاهد من توجيه تهم جنائية إليه على أساس شهادته أمام هيئة المحلفين الكبرى.

يجب موافقة قاض على منح الحصانة. يمكن للمدعي العام الحصول على الموافقة المسبقة للقاضي على منح الحصانة؛ أو يتم إحضار الشاهد أمام قاضي، بناء على طلب المدعي العام، يمنح دوماً الحصانة.

في حالة إصرارك على رفض الإجابة على الأسئلة قبل الحصول على الحصانة، يمكن للمدعي العام إحضارك أمام قاض والذي يقوم بدوره بأمرك بالشهادة. وفي حالة مواصلتك الرفض، قد يقوم القاضي بالأمر بسجنك بتهمة العصيان المدني. إن الشهود الذين يرفضون تقديم نماذج مادية، مثل عينات من خط اليد أو الشعر أو حضور طابور عرض أو مستندات، بناء على طلب هيئة محكمة كبرى، قد يتم سجنهم كذلك بتهمة العصيان المدني.

بينما لا يعد العصيان المدني جريمة، إلا أنه قد يؤدي إلى سجن الشاهد طوال مدة انعقاد هيئة المحلفين الكبرى. هذا ويمكن أن تستمر هيئة المحلفين الكبرى لمدة تصل إلى 18 شهراً، على الرغم من أن بعض هيئات المحلفين الكبرى "الخاصة" يمكنها الحصول على ثلا فترات إضافية تصل مدة كل منها ستة أشهر. إن الهدف من احتجاز شاهد متمرد هو إجباره على الإدلاء بشهادته. ومن ثم، قد يقوم بعض القضاء بالإفراج عن الشهود قبل انتهاء فترة هيئة المحلفين إذا كان من الواضح عدم وجود أي أمل في إدلاء الشاهد بشهادته.

ماذا يحدث إذا امتثلت إلى مذكرة إحضار أمام هيئة محلفين كبرى؟ (تـــابع ...)

يمكن للحكومة كذلك استخدام تهمة "العصيان الجنائي" ضد شهود هيئة المحلفين الكبرى غير المتعاونين. لا توجد عقوبة قصوى للعصيان الجنائي – فالحكم يعتمد على نحو مطلق على تقدير القاضي. بينما يهدف الاتهام بالعصيان المدني إلى إجبار الشاهد على الشهادة، فإن الاتهام بالعصيان الجنائي يهدف إلى معاقبة الشاهد على عرقلة العملية القانونية. وكما هو الحال مع أي جريمة أخرى، يستدعي العصيان الجنائي وجود مذكرات الاتهام والحق في الحصول على مساعدة محامي ودليل يتجاوز الشك المعقول. تعد التهم بالعصيان الجنائي نادرة للغاية.

إذا تم احتجازك، يمكنك القيام بصفة دورية بتقديم طلب تنص فيه على ما يلي: 1) السجن لن يجبرك على الشهادة، 2) احتجازك يعد عقابي تماماً ومن ثم هو غير دستوري. إذا ربحت أحد هذه الطلبات، سيتم الإفراج عنك.

يقوم بعض النشطاء بإعداد ملفات للاستعداد إذا تم استدعاؤهم أمام هيئة محلفين كبرى، وهو ملف مدون فيه إيمانك الراسخ ضد التعاون مع إجراءات هيئة المحلفين الكبرى، ويستخدم هذا الملف كدليل على أن الاتهام بالعصيان الجنائي لم يود نفعاً في إجبارك على الشهادة، ومن ثم يساعدك في الحصول على الإفراج.

ما الذي يحدث عقب المثول أمام هيئة محلفين كبرى؟

ما يحد تحت إطار إجراءات هيئة المحلفين الكبرى يعد أمراً سرياً. حيث تستند الحكومة على هذه السرية لبث الخوف وزعزعة الثقة في مجتمعات النشطاء. ولقد نجح بعض النشطاء في القضاء على هذا الخوف وعدم الثقة من خلال نشر الأسئلة التي تم توجيهها إليهم من قبل المدعي العام والإجابات التي قدموها. إذا كنت تفكر في التصرف على هذا النحو، يتعين عليك أولاً التحد مع محامي لتتأكد من عدم إثارة المزيد من المشكلات بدلاً من حل البعض منها.

اعتبارات خاصة لغير المواطنين

غير المواطنين هم أشخاص لا يحملون الجنسية الأمريكية، ومن بينهم السائحين والطلاب وغيرهم من أشخاص متواجدين في الولايات المتحدة بموجب تأشيرات مؤقتة أو برامج الإعفاء من التأشيرة أو المقيمين الشرعيين أو اللاجئين أو هؤلاء الذين بدون موقف هجرة شرعية. يتشارك غير المواطنين في الولايات المتحدة في كثير من الحقوق الدستورية التي يتمتع بها المواطنون. إلا أنه ثمة بعض الاستثناءات لهذه القاعدة، ويتعين على غير المواطنين الممارسين لأنشطة سياسية إدراك تلك الحقيقة والوعي بتلك الاعتبارات الخاصة. ومع ذلك، يجب على غير المواطنين عدم تجنب النشاط السياسي تماماً بدافع من خوف لا مبرر له من قمع الحكومة.

الخطاب والتبعيات السياسية

في أغلب الحالات، تتعامل الحكومة مع الخطاب الصادر عن غير المواطنين على نفس النحو الذي تتعامل به مع المواطنين. فلا يجوز معاقبة غير المواطنين جنائياً على الخطاب الذي قد يخضع للحماية إذا صدر عن مواطن. وبالمثل لا يمكن مقاضاة غير المواطنين على الحديث إذا قيل من قبل مواطن.

ومع ذلك، تتمتع الحكومة بسلطات واسعة النطاق تتيح لها حجب إعانات الهجرة (مثل سبل الإغاثة التقديرية أو التجنيس)، بل قد تقوم بتحريك دعوى طرد استناداً على خطاب صادر عن أجنبي. فليس من الواضح إذا كان في وسع الحكومة طرد شخص أجنبي أو تحجب عنه الإعانات التقديرية نتيجة لخطاب أو وجود علاقة سياسية فقط.

منذ خمسين عاماً مضت وجدت بعض المحاكم أن الحكومة تستطيع، ولكن قانون التعديل الأول قد تغير جذرياً منذ ذلك الحين، وانقسمت المحاكم الآن بشأن ما إذا كانت هذه القاعدة تشكل قانوناً جيداً أم لا. من الناحية العملية، نادراً ما تقوم الحكومة بترحيل شخص على أساس الحوار أو الجمعية فقط لا غير. ولكن يُسمح للحكومة بتفعيل قوانين الهجرة بشكل انتقائي. على سبيل المثال، يمكن للحكومة ترحيل غير المواطنين بسبب انتهاك قانون الهجرة. (مثل البقاء بعد انتهاء مدة التأشيرة، أو العمل بدون تصريح) حتى لو كان دافع الحكومة في بدء إجراءات الترحيل هو خطاب ألقاه غير المواطن أو انتمائه لجمعية سياسية.

الخطاب والتبعيات السياسية (تابع ...)

أخيراً، يتعين على طالبي الإقامة الدائمة والجنسية عرض قائمة بالمنظمات التي عملوا لديها. يُنصح غير المواطنين من النشطاء السياسيين باستشارة محامي هجرة قبل التقدم لطلب تغيير الحالة لأن بعض الجمعيات قد تتسبب في مشاكل أثناء إجراء طلبك.

عمليات التفتيش والاعتقال

يتمتع غير المواطنين بشكل كبير بنفس تحصينات التعديل الرابع ضد التفتيش والاعتقال غير المبرر الذي يقوم به المواطنون. يجب أن يتم تفعيل القانون من خلال الحصول على ضمان لإجراء أي تفتيش لغير المواطن أو ملكية غير المواطن فقط كما يجب القيام بتفتيش المواطن. يتم استبعاد دليل انتهاك التعديل الرابع من المحاكمة الجنائية لغير المواطن كما هو الحال بالنسبة للمواطنين.

لسوء الحظ، يُسمح بشكل عام باستخدام الدليل الذي تم الحصول عليه لانتهاك التعديل الرابع في إجراءات الهجرة. هذا يعني أنه يمكن للحكومة استغلال الدليل بشكل غير قانوني والذي لا يمكن استخدامه في الإجراءات الجنائية لغرض إجراءات الهجرة. من الممكن استبعاد دليل تم الحصول عليه من خلال انتهاكات مكشوفة خاصة للتعديل الرابع في إجراءات الهجرة.

كما يمكن للحكومة بشكل عام تفتيش وضبط أي شخص، مجموعة أو سيارة تسافر عبر الحدود أو في المطار.

حق التزام الصمت

يتمتع غير المواطنين بشكل عام بنفس الحق في التزام الصمت الذي يتمتع به المواطنون. في حالة الاستجواب من قبل عملاء تنفيذ القانون، يمكنك التزام الصمت ورفض الإجابة على أسئلتهم حتى لو قاموا بحبسك بشكل مؤقت أو اعتقالك. يمكن ببساطة عدم التفوه بشيء أو قول "أود التحدث إلى المحامي الخاص بي قبل أن أقول أي شيء إليكم" أو "ليس لدي ما أقوله لكم. سأتحدث إلى محامي وأجعله يتصل بك". لا توقع على شيء دون قراءته وفهم تبعات توقيعه جيداً.

هناك استثناء واحد لهذه القاعدة وهو إذا طلب ضابط الهجرة من غير المواطن تقديم معلومات بشأن وضع هجرته، ولكن حتى في هذا الموقف يمكنك الاستمرار في طلبك حضور المحامي قبل الإجابة على الأسئلة.
كما يتطلب القانون من غير المواطنين البالغين ممن معهم مستندات هجرة سليمة أن يحملوا تلك المستندات طوال الوقت. إذا طلب العميل منك المستندات ورفضت تقديمها، يمكن اتهامك بالمخالفة.

لا تظهر أبداً أوراق هجرة مزورة أو تدعي أنك مواطن أمريكي إذا لم تكن كذلك. بدلاً من هذا، يجب عليك التزام الصمت أو طلب محامي. إن الكذب على العميل الفدرالي تعد جريمة أكثر خطورة من المخالفة وعدم تقديم المستندات – من الأفضل عدم تقديم أي ورق عن تقديم مستندات مزورة. كما أن الادعاء الكاذب بأنك مواطن قد يحرمك من الحصول على الإقامة الشرعية أو المواطنة في المستقبل.

المحصـــــلة

كما سبق وذكرنا، تعد المعلومات المذكورة ضمن هذا الكتيب ليست سوى معلومات أولية حول حقوقك الأساسية. إن الهدف من هذا الدليل هو مساعدتك على إعداد نفسك ومنظمتك وزملائك من النشطاء على أن تكونوا مسلحين بالمعرفة وبالحماية في حالة ما جاء عميل يطرق بابك. وتذكر جيداً أن القوانين تختلف من ولاية لأخرى ــ لذا من الأحرى بك معرفة ولايتك وأن تكون على صلة بمحامي على معرفة جيدة بها.

نحن نأمل أن يكون هذا الكتيب بمثابة أداة نافعة لك ولمنظمتك أثناء سعينا لتحقيق عالم أكثر عدلاً على المستوى الاجتماعي.

للحصول على نسخ من هذا المنشور، تفضل بزيارة موقع http://ccrjustice.org/ifanagentknocks أو راسلنا مباشرة على iaak@ccrjustice.org

مصـادر إضـافية

حول ممارسات الأمن العام:

Security Culture: a Handbook for Activists

ثقافة الأمن: كتيب لكل ناشط: كتاب ممتاز بقلم نشطاء كنديون حول الدافع وراء بناء ثقافة أمنية وكيفية تحقيق ذلك.

http://security.resist.ca/personal/culture.shtml

Security Survival Skills, by the Collective Opposed to Police Brutality

مهارات البقاء الأمنية، توضيح لكيفية بناء ثقافة أمنية داخل مجتمعك من النشطاء بقلم مجموعة كندية.

http://www.why-war.com/fi les/Securite-eng-letter.pdf

War at Home

بقلم بريان جليك: كتاب مفصل حول تاريخ برنامج مكافحة التجسس (COINTELPRO) ويستعرض بعض النصائح الرائعة حول كيفية تجنب الشراك المشابهة وحماية نفسك ومجموعتك. نشر بواسطة مطبعة ساو إيند.

حول العملاء الحكوميين:

The Attorney General's Guidelines on FBI Undercover Operations

قواعد الحكومة الفدرالية بشأن ما يجوز للعملاء الفيدراليين المتخفيين فعله وما لا يجوز لهم فعله.

http://www.usdoj.gov/olp/fbiundercover.pdf

The Attorney General's Guidelines Regarding the Use of Confidential Informants

قواعد الحكومة الفدرالية بشأن ما يجوز للمخبرين فعله وما لا يجوز لهم فعله.

http://www.usdoj.gov/olp/dojguidelines.pdf

Security Practices and Security Culture

معلومات أساسية حول كيفية التعامل مع العمليات السرية وبعض النوادر الرائعة من عصر برنامج مكافحة التجسس.

http://aia.mahost.org/sec_cointelpro.htm

حول أمن الاتصالات الهاتفية:

Mobile Surveillance Primer

مصدر شامل متوفر على الإنترنت حول تقنيات الهواتف الخلوية وكيفية الوصول إليها وكيفية حماية المعلومات المخزنة عليها وحماية محادثاتك.

http://mobileactive.org/wiki/Mobile_Surveillance-A_Primer

حول خطابات الأمن القومي:

A Review of the FBI's Use of National Security Letters

صادر عن وزارة العدل: نظرة متعمقة في القانون المعني بخطابات الأمن القومي وكيف تم استخدامها منذ بدايتها.

http://www.usdoj.gov/oig/special/s0703b/fi nal.pdf

حول أمن الحاسب:

Computer Security Trainer's Guide

صادر عن Midnight Special Law Collective: دليل رائع بحق حول تنمية العادات الأمنية الجيدة الخاصة بالحاسبات بدلاً من الاعتماد على البرامج أو الحيل التقنية.

http://www.midnightspecial.net/materials/trainers.html

NGO in a Box: Security Edition

بواسطة Tactical Technology Collective and Front Line Human Rights Defenders: مجموعة إرشادية تهدف إلى مساعدة النشطاء ومسؤولي الإعلام المستقل على توفير الأمن الرقمي وحماية خصوصيتهم. تتضمن المجموعة أدلة حول أدوات التشفير والفيروسات وبرامج إزالة ملفات وبرامج التجسس وتخزين البيانات وحماية كلمة المرور وما إلى ذلك من معلومات. تتوافر المجموعة مجاناً على الإنترنت على موقع: http://security.ngoinabox.org

Security Practices and Security Culture

معلومات أساسية حول كيفية التعامل مع العمليات السرية وبعض النوادر الرائعة من عصر برنامج مكافحة التجسس.

http://aia.mahost.org/sec_cointelpro.htm

حول المراقبة مرتفعة التقنية:

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society

بواسطة: ACLU، دراسة حول التاريخ الحديث لكاميرات المراقبة والتقنيات الأخرى.

http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf

حول هيئات المحلفين الكبرى:

Grand Jury Trainers Guide

بواسطة: Midnight Special Law Collective، شرح توضيحي لهيئة المحلفين الكبرى – بدءًا من الاتصال الأول بالعملاء الفدراليين إلى جلسة الاستماع أمام هيئة المحلفين الكبرى ذاتها – وكيفية حماية نفسك ومجموعتك إذا ما تم استدعاؤك أمام إحدى الهيئات.

http://www.midnightspecial.net/materials/trainers.html#gj

بيان إنكار المسؤولية: هذا الكتيب للأغراض الإعلامية فقط ولا يمثل نصيحة قانونية. يهدف مركز الحقوق الدستورية إلى عرض وصف عام للقضايا القانونية والعملية التي قد يواجهها النشطاء التقدميون أو الراديكاليون. وتجدر الإشارة هنا إلى أن كل شخص تحيط به ظروف خاصة ومختلفة عن غيره، وتلك الاختلافات الضئيلة يمكن لها تثمر عن إجابات شديدة التباين على الأسئلة المقدمة هنا. للحصول على إجابات وافية عن مشكلات أو قضايا أو أسئلة قانونية محددة، احصل على نصيحة محامي مؤهل في منطقتك.

الإقرارات والتصديقات

مركز الحقوق الدستورية
Broadway, 7th Floor 666
New York, NY 10012
www.CCRJustice.org / (212) 614-6464

إن مركز الحقوق الدستورية مكرس تماماً لتعزيز وحماية الحقوق التي يكفلها دستور الولايات المتحدة الأمريكية والإعلان العالمي لحقوق الإنسان. تم تأسيس المركز عام 1966 على يد مجموعة من المحامين الذين مثلوا الحركات المنادية بالحقوق المدنية في الجنوب، وهو منظمة تعليمية لا تهدف إلى الربح، ملتزمة نحو الاستخدام الإبداعي للقانون كقوة إيجابية لتحقيق التنغيير الاجتماعي. تفضل بزيارة: www.ccrjustice.org

المؤلف الرئيسي، ماثيو شتروجر، محام في فريق عمل مركز الحقوق الدستورية. تم إعداد كتيب" إذا جاء عميل يطرق الأبواب" بواسطة موظفي ومحرري مركز الحقوق الدستورية، ومن بينهم لورين ميلوديا وراشيل ميروبول وأليسون روه بارك وقعيد جاكوب وجيف دوتش وأروا فداء حسين وكاثي جيفوني وتوني هولنيس وكارولين هسو وجيسيكا جواريز وكينيث كروشر وديفيد ماندل–أنتوني وكريستينا ستيفنسون.

ترجمة النص إلى اللغة العربية: Morningside Translations
تصميم الغلاف من عمل روبرت تروجيلو (2011)
التصوير بواسطة مادي ميلر (صفحات، 5 و9 و15)
التصوير بواسطة SSGT رينولدو رامون، USAF (صفحة 21)
التصوير بواسطة جاريكتوزنيسكي (صفحة 36)
الخطوط المستخدمة: AXT–Lakhdar (النص الرئيسي)، TheMixArab (العناوين)
الأيقونات بواسطة: pixel–mixer.com
التصميم: قائد جاكوبس، أحمد فولة

إذا جاء عميل يطرق الأبواب

centerforconstitutionalrights

on the front lines for social justice