هل يستطيع أمن الحدود تفتيش الـأجهزة الإلكترونية الخاصة بك؟ الموضوع مُعقد.

إيشا بنداري، محام، ACLU (اتحاد الحريات المدنية الامريكي) مشروع التعبير و الخصوصية و التكنولوجيا
و نيثان فريد وايسلر، محام، ACLU مشروع التعبير و الخصوصية و التكنولوجيا
و نوعة ياخوت، ACLU استراتيجي تواصل
14 مارس 2017

لقد وصلت إلينا تساؤلات كثيرة عن قانونية قيام موظفي الحدود بتفتيش الأجهزة الإلكترونية للمسافرين في المطارات الدولية و المنافذ الحدودية الأخرى. مع الأسف، الإجابة ليست بسيطة.

طالما ما ادعت الحكومة بأن التعديل الرابع الذي يمنع التفتيشات الغير مرخصة لا ينطبق عند الحدود. لا تتفق الACLU مع هذه المسألة بشكل عام، و خصوصا فيما يتعلق بالأجهزة الإلكترونية مثل الهواتف الذكية و الحواسب المحمولة. تقوم هواتفنا الذكية بتخزين تفاصيل حاسباتنا الخاصة باتصالاتنا و حياتنا العملية و الأماكن التي تواجدنا بها و عادات تصفحنا على الإنترنت. تقوم برسم صورة تفصيلية لحياتنا الخاصة أكثر من لنقول حقيبة سفر.

و قد أدركت المحكمة الدستورية هذه الحقيقة عندما قامت بالحكم سنة 2014 بأن الدستور يُلزم الشرطة الحصول على إذن لتفتيش الهاتف الذكي الخاص بشخص ما تم اعتقاله. و كما قامت الACLU في كثير من قضايا المحاكم بالمجادلة بأنه لا مبرر بعدم تطبيق الدستور الذي يحمي من التفتيشات الغير مرخص بها عندما نسافر دولياً باعتبار سعة انتشار هذه الأجهزة و قابليتها المتزايدة في رصد التفاصيل الدقيقة لحياتنا الخاصة.

مع الأسف لا تتفق الحكومة مع هذا و القانون الذي سيحسم في الأمر لا يبدو أنه سيتم الفصل به عن قريب. و بسبب الآثار عالية الخطورة المترتبة على هذه النوعيات من التفتيشات، و في وسط دلالات تقترح زيادة حدوثها، فإنه من المهم فهم و استعراض الموقف حتى يتسنى لك الوصول إلى قرارات سليمة لك قبل السفر.

يعرض هذا المصدر سيناريوهات انتقائية أساسية محتملة خاصة بالتفتيشاتعلى الجهاز الإلكتروني. و للتعرف أكثر على قضايا الحريات المدنية الأخرى التي عادة ما تحدث عند الحدود، اضغط هنا. و إن كنت تعتقد بأنه تم انتهاك حقوقك الدستورية، اذكر لنا ماذا حدث و قم بملء هذا النموذج.

ماذا يحدث إذا طلب مني موظف الحدود تسليم جهازي؟

تدعي الحكومة أن لديها السلطة لتفتيش جميع الأجهزة الإلكترونية بغض النظر عن وضعك القانوني بالبلد أو ما إذا كان لديها أي قناعات للاشتباه بتورطك في جريمة. يمكنك أن تقول بأنك لا توافق على مثل هذا التفتيش و لكن مع الأسف هذا لن يمنع موظفي الCBP(الجمارك و حرس الحدود) من أخذ هاتفك المحمول.

و إذا قمت بإعطاء موظفي حماية الجمارك و الحدود كلمة السر الخاصة بهاتفك المحمول (أو إذا لم يكن لديم كلمة سر) فربما يقومون بإجراء ما يسمى ب "تفتيش سطحي" لحظي. و ربما أيضاً يقومون بتحميل جميع مكونات جهازك و حفظ نسخة من بياناتك. و طبقاً لسياسات الCBP لسنة 2009 فإنه لا يتوجب عليهم إعادة جهازك لك قبل أن تترك المطار أو منفذ حدودي آخر و ربما يقرروا إرساله إلى البحث الجنائي للمزيد من التفتيش. باستثناء "المواقف التخفيفية" ، فإنهم يدعون أن لديهم السلطة باحتجاز الجهاز لمدة خمسة أيام- و بغض النظر فإن عبارة "المواقف التخفيفية" هي عبارة غير محددة في هذا السياق و يمكن مد الفترة إلى سبعة أيام متزايدة. لقد وصلتنا تقارير عن هواتف تم احتجازها لأسابيع أو حتى شهور.
و كنتيجة لهذه السياسة فإن حتى المعلومات الخاصة المتعارف عليها دوليا –مثل محادثاتك مع محاميك- لا يتم حمايتها كفاية عند الحدود. إذا كنت تمتلك أي معلومات تحت حماية المحامي- العميل، فإنه يجب عليك إخبار موظف الCBP الذي تتعامل معه. مع الأسف فإن كل ما سيقوم أو ستقوم بفعله طبقا لسياسة الوكالة هو "استشارة" المدير قبيل التفتيش.

لا يتمتع الصحافيون الذي يحملون معلومات حساسة عن عملهم أو مصادرهم بالحماية الكافية. تعليمات الCBP توجه بأن "المعلومات المتعلقة بالعمل التي يحملها الصحفيون سيتم التعامل معها طبقاً للقانون الفدرالي و سياسة الCBP "- و لكن المعني غير واضح. على الصحفيون الذين شعروا بأن حقوقهم انتهكت عند الحدود إخبارنا و على هؤلاء الذين سيسافرون استشارة المكاتب القانونية بمؤسساتهم أو المؤسسات الإعلامية.

إذا قمت بترك المطار أو نقطة تفتيش حدودية أخرى بدون جهازك، تأكد من الحصول على إيصال يحتوي على معلومات عن جهازك و بيانات الاتصال للمتابعة. و إذا، و بعد إجراء البحث الجنائي، و عدم وجود أي سبب محتمل بأن الجهاز يحتوي على أدلة تورط في جريمة، فإن الحكومة تقول بأنها ستدمر أي معلومات قامت بنسخها في خلال 21 يوماً. و لكن يتوجب التنبيه هنا. بأن الCBP يمكن أن تقوم بحفظ أي مذكرات تم أخذها خلال البحث في جهازك أو أي تحقيقات تمت معك عند الحدود.

هل يتوجب علي أن أقوم بإدخال كلمة السر لفتح جهازي؟

إن وضعك القانوني في البلد قد يحدد قرارك فيما ستفعله إذا طلب منك إعطاء كلمة السر لفتح جهازك.

إذا كنت مواطن، فإنه لا يجب منعك من دخول البلد إذا رفضت الإذعان لطلب فتح جهازك أو إعطاء كلمة السر. و لكن يمكن أن يتم حجزك لفترة أطول أو الحجز على جهازك و عدم إرجاعه لك لأسابيع أو شهور. و نفس الشيء صحيح بالنسبة لهؤلاء الذين دخلوا إلى الولايات المتحدة كمقيمين دائمين قانونين و بقوا على وضعهم- لا يمكن إلغاء بطاقاتهم الخضراء بدون جلسة استماع أمام قاضي هجرة. إن كنت لست مواطناً و قلق بشأن تفتيش جهازك، فيتوجب عليك استشارة محام هجرة حول الظروف الخاصة بك قبل السفر.

إلا أنه تكون هناك مخاطرة لحاملي تأشيرات الدخول و السائحين من الدول المعفية من تأشيرة الدخول بأن يتم منعهم من الدخول في حالة رفضهم إعطاء كلمة السر، و يتوجب عليهم دراسة هذه المخاطرة قبل اتخاذ أي قرار. تقوم إدارة الأمن الوطني حالياً بدراسة وضع سياسة تلزم الزائرين من بعض البلدان إعطاء كلمة السر لمواقع التواصل الاجتماعي الخاصة بهم للموافقة على إعطاء تأشيرة سفر إلى الولايات المتحدة الأمريكية. (تعارض ACLU هذا المقترح).

حتى ما إذا كنت مواطناً أم لا، فنحن دائما نوجه بقيامك بإدخال كلمة السر بنفسك و عدم كشفها لموظف الCBP. مع ذلك قد يطلبوا منك الكشف عنها لهم، و لكن الحذر واجب. إذا قمت بإعطاء كلمة السر فمن المرجح أن يتم إدراكها في قاعدة بيانات الحكومة، لذا قم بتغييرها بمجرد وجود الفرصة لذلك و تأكد من عدم استخدام كلمة السر هذه مع أي حساب آخر.

ماذا يجب علي فعله لأصبح جاهزاً؟

فيما يلي عرض لبعض الاحتياطات التي عليك اتخاذها في التحضير لرحلتك للتأكد من سير الأمور على ما يرام بقدر المستطاع:

- **إحمل في سفرك أقل بيانات و أقل أجهزة بقدر المستطاع.** قلّما حملت معك قلّما كان التفتيش. يمكن أن تأخذ معك هاتف ذكي خاص بالسفر أو جهاز حاسوب محمول لا يحتوي على معلومات خاصة أو حساسة. يمكن أيضاً أن تقوم بشحن أجهزتك مسبقاً. (عليك الإنتباه بأن ال CBPمن سلطتهم تفتيش أي طرود دولية لذلك من المفضل تشفير أي أجهزة قبل شحنها). تذكر بأن البحث الجنائي على الجهاز من شأنه أن يُرجع البيانات المحذوفة و البيانات الخلفية و ملفات أخرى.

- **قم بتشفير الأجهزة باستخدام كلمات سر قوية و مميزة و إغلاق الأجهزة قبل عبور الحدود.** للحصول على مصادر جيدة في كيفية فعل هذا إضغط هنا.

- **قم بخفظ البيانات الحساسة في حسابات تخزين ضوئية.** لا تحتفظ بنسخة من البيانات في متعلقاتك المادية و قم بتعطيل أي تطبيقات متصلة بحسابات ضوئية قد قمت بتخزين إتصالات حساسة أو ملفات بها. (لا يوجد سياسة ل CBPمتعلقة بما إذا كان من حق الموظفين الضغط على تطبيقات و بحث البيانات المخزنة بالحساب الضوئي. بينما يكون هذا النوع من التفتيش الغير مرخص خارج سلطة الحكومة عند الحدود، فإننا لا نعلم رؤيتهم لهذه المسألة.)

- **قم بتحميل الصور الحساسة الموجودة على الكاميرا الخاصة بك بجهاز الحاسوب الخاص بك المؤمن بكلمة سر أو حسابك الضوئي.** الكاميرات الرقمية لا توفر تخزين تشفيري، لذا يجب عليك التفكير في نسخ صورك في مكان آخر و مسحها من على الكاميرا و إعادة تشكيل البيانات من على بطاقة ذاكرة الكاميرا.

و إلى أن تصل المحكمة الدستورية إلى قرار بشأن سقف الصلاحيات الدستورية الممنوحة للحكومة عند الحدود، فإنه من الصعب حسم التساؤلات حول سلطة الحكومة في القيام بمثل هذه التفتيشات. قامت المحاكم الأدنى بإصدار أحكام متضاربة فيما يختص بما إذا كان الاشتباه الفردي شرط لإجراء مثل هذا التفتيش. فعلى سبيل المثال فإن الدائرة القضائية التاسعة، و التي تغطي ولايات غربية عديدة، تقتضي وجود اشتباه معقول لإجراء "جنائي" على جهاز تم توقفيه، و لكنها لم تضع حدوداً حول التفتيشات السطحية اللحظية.

من المصيري أن تقوم محاكم أكثر بالبت في المسألة، و خصوصاً أن تفتيشاتالأجهزة عند الحدود في تزايد. التقارير الحديثة تشير إلى أنه في عام 2016، تم تفتيش حوالي 24000 جهاز إلكتروني، و هي قفزة كبيرة من حوالي 5000 جهاز تم تفتيشهم في عام 2015. إن وتيرة التفتيشات مستمرة في التسارع، وبتقرير إدارة الأمن الوطني فإنه تم إجراء تفتيش على 5000 جهاز في فبراير 2017 فقط.
مع تزايد ممارسة موظفي الحدود سلطات أكبر و التي لم تكن محسومة بشكل كافٍ من المحاكم، فإنه تزداد الحاجة العاجلة إلى وضع حمايات واضحة. و فينفس الوقت، فإن على المسافرين أخذ الاحتياطات التي يشعرون أنها مناسبة لهم.