حضور در اعتراضات

www.ssd.eff.org

گردآوری و ترجمه:

حضور در اعتراضات

اکنون، بیش از هر زمان دیگری، شهروندان باید بتوانند کسانی را که در قدرت هستند پاسخگو نگه دارند و از طریق عمل اعتراض، دیگران را الهام بخشند

حفاظت از دستگاه‌های الکترونیکی و دارایی‌های دیجیتالی شما قبل، حین و بعد از اعتراض برای حفظ امنیت خود و اطلاعات شما، و همچنین انتشار پیام شما، حیاتی است. سرقت، آسیب، مصادره یا حذف اجباری رسانه می‌تواند توانایی شما را در انتشار تجربیات خود مختل کند. در عین حال، کسانی که در اعتراض شرکت می‌کنند ممکن است مورد تفتیش یا بازداشت قرار گیرند یا حرکات و ارتباطات آنها مورد نظارت قرار گیرد.

به یاد داشته باشید که این نکات پیشنهادات کلی برای امنیت داده‌ها هستند و مشمول مشاوره یا وکالت حقوقی نمی‌شوند. اگر نگرانی‌های حقوقی خاصی دارید، از یک وکیل مجوزدار مشورت بگیرید.

قبل از شرکت در اعتراضات

• رمزگذاری کامل دیسک را روی دستگاه خود فعال کنید

رمزگذاری کامل دیسک اطمینان حاصل می‌کند که پرونده‌های سراسر دستگاه شما رمزگذاری شده‌اند. این یک نوع رمزگذاری است که داده‌ها را در حالت سکون محافظت می‌کند - که نباید با «رمزگذاری در حین انتقال» اشتباه گرفته شود، که داده‌هایی را که از طریق اینترنت منتقل می‌شوند، محافظت می‌کند. رمزگذاری کامل دیسک می‌تواند از همه چیز از پایگاه داده محلی پیام‌های متنی شما تا گذرواژه‌های ذخیره شده در مرورگر شما محافظت کند. اگر دستگاه شما توسط پلیس مصادره شود یا گم شود یا دزدیده شود، رمزگذاری کامل دیسک می‌تواند از داده‌های ذخیره شده در دستگاه شما محافظت کند. موقعیت‌های اعتراض اغلب غیرقابل پیش‌بینی هستند، بنابراین گم شدن تلفن یک احتمال قریب به یقین است.

Android و iOS مدت‌هاست که قابلیت‌های رمزگذاری کامل دیسک را در دستگاه‌ها تعبیه کرده‌اند. این‌ها باید با یک رمز عبور قوی محافظت شوند: ۸-۱۲ کاراکتر تصادفی که به راحتی می‌توانید آن را به خاطر بسپارید و هنگام باز کردن قفل دستگاه خود تایپ کنید. اگر دستگاه‌ها با رمز عبور قوی محافظت نشده باشند، رمزگذاری ممکن است با استفاده از حمله brute-force آسان‌تر شکسته شود. iPhone 5s و بعد از آن دارای سخت‌افزار تخصصی برای محافظت در برابر این نوع حمله هستند، اما دور زدن‌هایی برای این محافظت همچنان در حال توسعه هستند و بنابراین یک رمز عبور پیچیده و قوی هنوز بهترین practice است.

رمزگذاری دستگاه شما به احتمال زیاد مموری کارت‌های خارجی مانند SD یا فلش را رمزگذاری نمی‌کند. شما باید این‌ها را به صورت جداگانه رمزگذاری کنید و ممکن است اصلاً قادر به رمزگذاری آنها نباشید. ممکن است بخواهید با استفاده از یک برنامه مرورگر فایل، مکان فایل‌ها را در دستگاه خود بررسی کنید یا مموری کارت خارجی را به طور کامل از دستگاه خود حذف کنید.

علاوه بر این، بسیاری از دوربین‌های دیجیتال قادر به رمزگذاری نیستند. فرض بر این است که عکس‌ها و فیلم‌های گرفته شده با دوربین‌های دیجیتال بدون رمزگذاری ذخیره می‌شوند، مگر اینکه صریحاً ذکر شده باشد.

- حذف قفل اثر انگشت و FaceID

امروزه، هم iOS و هم Android به کاربران اجازه می‌دهند دستگاه‌های خود را با اثر انگشت خود باز (و رمزگشایی) کنند، و مدل‌های FaceID iPhone X و بعدی به کاربران امکان انجام این کار را با تشخیص چهره می‌دهند. در حالی که این تنظیمات ممکن است به عنوان راه‌های convenient برای لذت بردن از مزایای رمزگذاری کامل دیسک جذاب به نظر برسند، فعال کردن آنها به این معنی است که یک افسر می‌تواند شما را با اثر انگشت یا صورت خود مجبور به باز کردن قفل دستگاه خود کند. در موقعیت‌های اعتراض به ویژه - یا در هر موقعیت دیگری که ممکن است بیشتر در معرض درخواست دولت برای جستجوی تلفن خود (مانند گذرگاه مرزی) باشید - ما پیشنهاد می‌کنیم این قابلیت را غیرفعال کنید.

مراقب باشید که در عکس‌ها و فیلم‌های خود سایر معترضان را قرار ندهید

اگر از افراد حاضر در اعتراض عکس یا فیلم می‌گیرید، مراقب باشید که چه چیزی را منتشر می‌کنید. اگر عکس‌هایی را به صورت آنلاین منتشر کنید که چهره‌های معترضان یا ناظران را می‌توان شناسایی کرد، ممکن است نیروهای انتظامی یا ناظران آنها را ردیابی کرده و دستگیر یا مورد آزار و اذیت قرار دهند. چهره افراد را در تصویر محو کنید. می‌توانید عکس‌ها را در برنامه های ویرایش عکس پیش‌فرض Android یا iOS ویرایش کنید. مطمئن شوید که سایر ویژگی‌های شناسایی مانند خالکوبی یا لباس‌های منحصربه‌فرد را نیز سیاه‌کنید یا محو کنید (محو کردن را می‌توان گاهی اوقات برگشت، بنابراین اگر گزینه دارید، سیاه کردن بهتر است). یک ابزار مفید به نام Image Scrubber وجود دارد که می‌توانید از آن در دستگاه‌های تلفن همراه یا دسکتاپ استفاده کنید.

حذف داده‌های EXIF از عکس‌ها

هنگامی که آماده ارسال عکس‌های خود هستید، اگر نمی‌خواهید اطلاعات شخصی شناسایی را فاش کنید، عاقلانه است که داده‌های EXIF موجود در پرونده‌های تصویر را پاک کنید. داده‌های EXIF در عکس‌ها می‌تواند شامل اطلاعاتی مانند مدل دوربینی که عکس با آن گرفته شده است، زمان و مکان دقیقی که عکس گرفته شده است و حتی نام شما باشد.

گزینه ۱: هرگونه داده EXIF اصلی را با انتقال عکس به یک رایانه رومیزی، گرفتن اسکرین شات از تصویر و ارسال اسکرین شات به جای عکس اصلی حذف کنید.

گزینه ۲: همچنین می‌توانید عکس را در دستگاه تلفن همراه خود اسکرین

شات بگیرید تا داده‌های EXIF حذف شوند، اما کیفیت تصویر ممکن است به اندازه عکس اصلی بالا نباشد. سپس می‌توانید آن اسکرین شات را به جای عکس اصلی ارسال کنید.

گزینه ۳: یک نسخه از عکس را از طریق برنامه Signal (که هنگام ارسال تصاویر داده‌های EXIF را حذف می‌کند) برای خود ارسال کنید، سپس تصویر ارسال شده را برای ارسال دانلود کنید.

مواردی که باید هنگام سفر به و از محل اعتراض به آنها توجه داشته باشید

- موارد مربوط به رانندگی

سیستم‌های خواننده پلاک خودروی خودکار (ALPR) به طور خودکار پلاک های خودروها را در حال رانندگی در یک منطقه ثبت می‌کنند، همراه با زمان، تاریخ و مکان دقیقی که با آنها مواجه شده‌اند. این فناوری اغلب توسط نیروهای انتظامی در ایالات متحده و بسیاری از کشورهای دیگر استفاده می‌شود، یا توسط شرکت‌های خصوصی مانند Vigilant و MVTrac به کار گرفته می‌شود که سپس داده‌های پلاک خودرو را با نیروهای انتظامی و سایر ذینفعان به اشتراک می‌گذارند. این داده‌ها در پایگاه‌های داده‌های بزرگی ذخیره می‌شوند و برای مدت‌های طولانی نگهداری می‌شوند. اساساً، می‌توان موقعیت شما را بر اساس سابقه رانندگی هر وسیله نقلیه‌ای که به شما ثبت شده است، ردیابی کرد، و محدودیت‌های قانونی بسیار کمی در مورد نحوه جمع‌آوری، دسترسی، اشتراک‌گذاری و نگهداری این داده‌ها وجود دارد.

• موارد مربوط به حمل و نقل عمومی

هنگام سفر به و از محل اعتراض مراقب باشید. اگر از روش‌های پرداخت یا کارت‌های حمل‌ونقل عمومی استفاده می‌کنید که به شما مرتبط هستند، ممکن است نیروهای انتظامی بتوانند تعیین کنند که شما در اعتراض شرکت کرده‌اید و حرکات شما را ردیابی کنند. اگر ترجیح می‌دهید حرکات و ارتباطات شما خصوصی باقی بماند، از روش‌های جایگزین حمل‌ونقل عمومی استفاده کنید.

اگر می‌توانید، پیاده یا دوچرخه‌سواری را برای رفتن به و از محل اعتراض در نظر بگیرید تا در معرض این نوع ریسک‌های جاسوسی قرار نگیرید.

تنظیمات تلفن خود را تغییر دهید

برای کاهش خطر اینکه کسی از طریق تلفن شما موقعیت شما را ردیابی کند، به تنظیمات تلفن خود بروید، حالت هواپیما را روشن کنید و Location Services، Wi-Fi و Bluetooth را غیرفعال کنید. اگر از یک تلفن Android استفاده می‌کنید، باید به حساب Google خود نیز بروید و Location History را غیرفعال کنید. این باید اطمینان حاصل کند که دستگاه شما در طول مدت حضور شما در اعتراض، انتقال نمی‌یابد و از ردیابی موقعیت شما جلوگیری می‌شود

با این حال، حتی زمانی که حالت هواپیما روشن است و Location Services، Wi-Fi و Bluetooth غیرفعال هستند، برنامه‌ها ممکن است بتوانند موقعیت GPS شما را ذخیره کنند و آن را پس از اتصال مجدد به اینترنت ارسال کنند. تنها راه اطمینان از این امر که این اتفاق نمی‌افتد، خاموش کردن کامل تلفن است.

روشن کردن حالت هواپیما و غیرفعال کردن Wi-Fi همچنین به این معنی

است که نمی‌توانید با دوستان خود پیامک یا تماس بگیرید، بنابراین در این مورد برنامه‌ریزی کنید. قبل از رفتن به اعتراض، با دوستان خود در مورد مکانی که می‌توانید اگر جدا شوید با یکدیگر ملاقات کنید، توافق کنید.

اگر به استفاده از GPS برای ناوبری نیاز دارید، از یک برنامه نقشه‌برداری آفلاین مانند Organic Maps استفاده کنید. همچنین می‌توانید قبلاً یک نقشه از منطقه اعتراض را دانلود کنید.

بعد از اعتراض

اگر دستگاه شما مصادره شد

اگر دستگاه شما مصادره شده است، ممکن است راه قانونی برای بازیابی آن داشته باشید. در ایالات متحده، وکیل شما می‌تواند درخواست بازگرداندن اموال شما را ارائه دهد اگر در پرونده‌ای در حال رسیدگی به عنوان مدرک نگهداری نشود. اگر پلیس معتقد باشد که مدرکی از جرم در دستگاه الکترونیکی شما یافت شده است، از جمله در عکس‌ها یا فیلم‌های شما، سپس پلیس می‌تواند آن را به عنوان مدرک نگه دارد. آنها همچنین ممکن است تلاش کنند مالکیت دستگاه الکترونیکی شما را به پایان برسانند، اما می توانید چنین مصادره دارایی را در دادگاه به چالش بکشید.

همچنین می‌توانید دسترسی را برای برخی از خدماتی که در دستگاه شما وارد شده‌اند، لغو کنید. به عنوان مثال، در توییتر، اگر به Settings and privacy -> Apps and devices بروید، می‌توانید دسترسی را برای دستگاه‌هایی که اجازه اتصال به حساب توییتر شما را دارند، لغو کنید. برای سایر خدمات، فقط تغییر رمز عبور یا عبارت عبور باعث می‌شود که برنامه برای خروج از

سیستم درخواست شود. اما مراقب باشید که لغو دسترسی نیروهای انتظامی ممکن است شما را در معرض اتهام ممانعت از اجرای عدالت یا تخریب مدارک قرار دهد. قبل از تصمیم‌گیری در مورد نحوه ادامه کار، همیشه باید ابتدا با وکیل خود صحبت کنید. خدمات آنلاین ممکن است سوابق ورود اخیر به حساب شما را ارائه دهند. اگر نگران هستید که دستگاه شما برای دسترسی به حساب‌ها بدون رضایت شما استفاده می‌شود، ممکن است مفید باشد که بررسی کنید که آیا چنین سوابقی در دسترس هستند و بر آنها نظارت کنید. اگر نیروهای انتظامی دستگاه شما را مصادره کنند، ممکن است از یک ابزار «forensic» مانند Cellebrite برای تلاش برای استخراج داده‌ها از دستگاه شما، مانند تصاویر، مخاطبین، پیام‌ها و سابقه مکان استفاده کنند. این احتمال بیشتر است که اگر تلفن شما قدیمی یا رمزگذاری نشده باشد، موفقیت‌آمیز باشد. به همین دلیل، مهم است که حداقل داده را با خود حمل کنید و از قوی‌ترین سطح رمزگذاری در موقعیت‌های پرخطر مانند اعتراض استفاده کنید.