مجموعة نصائح حول الخصوصية

كيف تؤثر التكنولوجيا في عملكم الحقوقي

https://datadetoxkit.org/en/privacy/protests/

سواءٌ أكنتم تعبرون عن وجهات نظرٍ معارضة عبر الوسائط الإلكترونية أم تقومون بالاحتجاج ميدانياً في الشوارع، فإنه لا ريب في أن التكنولوجيا قد غدت عاملاً أساسياً ومؤثراً في الكيفية التي بها تمارسون الاحتجاج. من إبداء الإعجاب Like بمنشور يعبر عما لديكم من شواغل أو القيام بمشاركته مع الغير Share، مروراً بتحديد أين تحضرون المظاهرات المحلية ومتى، وانتهاءً بتوثيق وتحميل الصور والحكايات التي تشهدونها بأنفسكم أو تصادفونها – فإنَّ **جهاز هاتفكم الذكي يمكن أن يكون حليفكم أو خصمكم**، بحسب الكيفية التي بها تستخدمونه.

إن دليل تنقية البيانات هذا يلقي نظرة فاحصة على بعض المخاطر والمنافع المحتملة لاستخدامكم الهاتف الذكي، ووسائل الاعلام الاجتماعية، وكذلك تطبيقات الرسائل؛ إن كنتم تقومون بأفعال تحمل صفة الاحتجاج. تجدون هنا أيضاً نصائح عملية لتكونوا **أكثر تنبُّهاً**، وعن كل ما يجب أن تحاذروه.

دعونا نلقي نظرة عن كثب!

بيان إخلاء المسؤولية: الأمر يتوقف على وضعك

اعتمادا على من تكونون، والعمل الذي تقومون به، والمكان الذي تقيمون فيه، قد تكون ثمة اعتبارات أو مخاطر معيّنة ينبغي أن تؤخذ في الاعتبار قبل اتباع أي نصيحة ترد في هذا الدليل أو أي دليل آخر. تأكدوا من أن تظلوا دوماً مطلعين على القوانين المحلية التي تعنيكم، واحرصوا على تقييم وضعكم الشخصي لما لذلك من تأثير على زيادة المخاطر المحدقة بكم أو الحد منها.

1. لا تقوموا بإدراج أسمائكم في قوائم الضيوف

التنصُّت الرقمي Digital listening طريقة تستخدم لمعرفة ما تهتمون به وتعتزمون القيام به استناداً إلى رصد نشاطكم العلنية على الإنترنت، سواء أكنتم تقومون بنشر رسائل غاضبة أو حزينة، أو تفضيلكم اللون الأزرق أو البرتقالي، أو آرائكم حول قضية ما. ويمكن لهيئات إنفاذ القانون أو الحملات السياسية أو الحكومات أو المسوِّقين التعاقد مع الشركات المتخصصة في التنصت الرقمي لتحديد المهتمين بقضايا بعينها أو الأشخاص الذين شاركوا في احتجاج معين. ويمكن أن يستهدف التنصت الرقمي شخصاً محدداً أو *مجتمعات بأكملها*.

والحقُّ أن الناس لا يُصعِّبون الأمر كثيراً على من يقومون بالتنصت – فهم إذ يرسلون ردودهم بتأكيد المشاركة في الاحتجاجات، ونشر Posting المعلومات حول الموقع الذي يتواجدون فيه أو عن عاداتهم، وقيامهم بضخّ الكثير من البيانات على الإنترنت؛ فإنهم يحوّلون مهمة القائمين بالتنصت الرقمي الى عملٍ في غاية البساطة. ثمة أمر أساسي واحد يمكنكم تغييره من الآن فصاعداً، ومن شأنه إحداث فرق كبير:

قرروا ما إذا كان إرسال تأكيد الحضور RSVP ضرورياً حقاً

يمكن لمواقع مثل فيسبوك Facebook و ميت أب Meetup أن تكون مصادر ممتازة للتعرف على الأحداث والمظاهرات في منطقتكم. لكن فكروا مرتين قبل إرسال تأكيد الحضور RSVP أو إظهار اهتمامكم بالحدث بطريقة أخرى، كالتغريد حول الموضوع أو نشر مواد عنه عبر موقع إنستغرام Instagram. ففي حين أنكم قد تكونون متحمسين لإبداء دعمكم لقضية ما، فإنَّ عليكم أن تتأكّدوا من تقييم المخاطر بمقتضى اعتباراتكم الشخصية. إذا كان لقائمة الضيوف أن تقع في الأيدي الخطأ، فكيف يمكن ذلك أن يؤثر عليكم؟

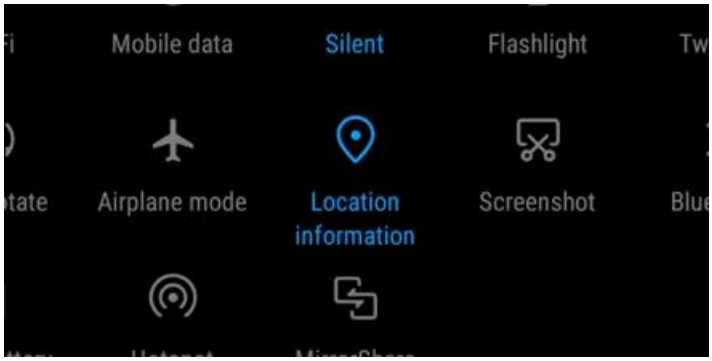
2. احذروا من تتبُّع الموقع

إنَّ بيانات الموقع location data قد تبدو محضَ نُتَفٍ عشوائية من المعلومات لا قيمة لها، إلا أنها قد تكون كافية لتمكين أحدهم من جمع القطع الصغيرة التي تخبر عنكم وأي نوع من الأشخاص تكونون. إذا لم تكن بيانات الموقع الخاصة بكم مؤمَّنة، فإنها يمكن أن تُخترق، أو تُسرَّب أو تُباع من قبل أي عدد من الأطراف الثالثة. إذا لم تكونوا ترغبون بأن تعلم شركاتٌ عشوائية أو هيئات فرض القانون أنكم حضرتم احتجاجاً، فانظروا في إمكانية إقفال خدمات الموقع الخاصة بكم. يعرض هذا *التحقيق الاستقصائي الذي نشرته صحيفة النيويورك تايمز* عدداً من الأمثلة على مدى السهولة التي يمكن لشخص ما أن يفهم حياتكم وعاداتكم من خلال معرفة موقعكم وحده.

يقوم جهاز هاتفكم الذكي بتتبع موقعكم من خلال عدد من الطرق. فلنلقِ نظرةً عن قرب عليها.

نظام التشغيل الأساسي لجهاز الهاتف

لعلكم لاحظتم أن معلومات الموقع في هاتفكم مفعَّلةٌ turned on بحكم الوضع الأصلي by default.



يمكن استخدام معلومات الموقع هذه من قبل أنظمة التشغيل أندرويد Android أو نظام آي أو إس iOS لعدد من الأسباب منها:

- إعلامكم بالطقس المحلي
- مشاركة الاتجاهات بسهولة من خلال تطبيق الخريطة map app
- وضع علامات tagging على الموضع الدقيق في الصور التي تلتقطونها
- إعادة توجيهكم إلى الصفحات المحلية لأحد المواقع الإلكترونية

قد يؤدي إيقاف تشغيل خدمات الموقع في هاتفكم إلى إطالة عمر البطارية. ويمكنكم إعادة تشغيل هذه الخدمة مرة أخرى بسهولة عندما تحتاجون إلى استخدام تطبيق الخريطة أو الطقس، على سبيل المثال.

الخطوات لنظام التشغيل أندرويد Android:

- الإعدادات Settings ←
- الأمن والموقع/ الموقع Security & Location / Location ←
- إيقاف تشغيل الموقع

الخطوات لجهاز آيفون iPhone:

- الإعدادات Settings ←
- الخصوصية Privacy ←
- خدمات الموقع Location services ←
- إيقاف تشغيل خدمات الموقع

التطبيقات Apps المُحمَّلة على جهاز الهاتف خاصتكم

قد يكون أمراً طبيعياً أن يتمكن تطبيق الخريطة، مثلاً، من الوصول إلى موقعكم. غير أنكم ربما ستتفاجؤون إذا علمتم عدد التطبيقات التي منحتموها إذناً بالوصول إلى موقعكم.

يمكنكم استعراض التطبيقات واحداً فواحداً وإغلاق الإذن الممنوح لتطبيق بعينه للوصول إلى خدمات الموقع. ابحثوا عن التطبيقات التي لا تحتاج إلى معرفة الموقع لكي تقدم الخدمة التي تُنتظر منها (هل يحتاج تطبيق الألعاب هذا إلى معرفة موقعكم؟) وكذلك عن التطبيقات التي لا تريدون لها أن تصل إلى موقعكم:

الخطوات لنظام التشغيل أندرويد Android:

- الإعدادات Settings ←
- التطبيقات Apps ←
- أذون التطبيقات App permissions ←
- قوموا بتحديد إمكانية وصول التطبيق إلى الموقع بحسب مقتضى الحال.

الخطوات لجهاز آيفون iPhone:

- الإعدادات Settings ←
- الخصوصية Privacy ←
- خدمات الموقع Location services ←
- قوموا بتحديد إمكانية وصول التطبيق إلى الموقع بحسب مقتضى الحال.

تعرَّفوا على المزيد من النصائح المتعلقة بمنح جهازكم بداية جديدة والتحكم في بيانات هاتفكم الذكي.

الأبراج الخلوية وشبكة الاتصال اللاسلكي (واي فاي)

أنتم مهَرةٌ في السيطرة على بيانات موقعكم – أحسنتُم صُنعاً! ولكن هل كنتم تعلمون أنه على الرغم من قيامكم بإيقاف تشغيل نظام التموضع العالمي GPS في هاتفكم، فإنه لا يزال في الإمكان تعقبكم من قبل الأبراج الخلوية القريبة أو شبكة الاتصال اللاسلكي (واي فاي)؟

وحتى إذا كنتم قد قمتم بتعطيل خدمة واي فاي وبيانات الهاتف النقَّال، فإن الرمز الموجود في أعلى شاشة الهاتف، والذي يشير إلى قوة الإشارة، يوضح أن هاتفكم يتواصل مع الأبراج الخلوية القريبة، الأمر الذي يكشف عن وجودك على مقربة من أماكنها... ويمكن لهيئات إنفاذ القانون استخدام هذه المعلومات في التعقب.

تشغيل وضع الطائرة

إذا كان هذا أمراً تقلقون بشأنه، ففي وسعكم تفعيل وضع الطائرة، وهو ما يخرجكم مؤقتاً من خريطة الأبراج الخلوية المحلية.

ولعلكم تتساءلون عن الجانب السلبي لهذا الإجراء؟ إنكم لن تتمكنوا من تلقي المكالمات أو الرسائل النصية أثناء تفعيل هذه الخاصية. ويمكن أيضاً أن تكون هيئات إنفاذ القانون ما تزال قادرة على معرفة المكان الذي تذهبون إليه، ويعتمد ذلك على عدد من العوامل (كالمعلومات الأخرى التي تم جمعها عنكم، وأنماط مواقعكم السابقة، والأشخاص الذين تكونون بصحبتهم، والتصوير لغايات المراقبة، وغير ذلك).

وفي حين لا يوجد الكثير مما يمكنكم القيام به للتصدي لهذا، فإن من المهم بالنسبة إليكم أن تعرفوا كيف تعمل هذه الشبكات لئلا تعرِّضوا أنفسكم للمخاطر على نحو لم تكونوا مدركين له. واعتمادا على عوامل مثل من تكونون، ما هو الوضع الخاص بكم، وأين تقيمون، فإنكم ستواجهون مخاطر مختلفة، وسيتعين عليكم تبعاً لذلك اتخاذ احتياطات مختلفة.

هل كنتم تعلمون؟ يواجه الجميع مخاطر مختلفة عند المشاركة في احتجاج. قوموا بالاطلاع على عدد من *التكتيكات التي توصي بها منظمة العفو الدولية لتأمين هاتفكم الذكي قبل المشاركة في احتجاج*، فهي تشتمل على قائمة من الاعتبارات التي يجب أن تأخذوها في الحسبان قبل مغادرة منزلكم. هل ينبغي لكم أن تأخذوا هاتفكم معكم أو تركه في المنزل؟ هل يمكنكم الحصول على هاتفٍ مسبق الدفع أم أن هذا سيوجد مخاطر جديدة (على سبيل المثال قد تكون مثل هذه الهواتف غير قانونية حيث تقيمون)؟

3. قوموا بجعل محاولة اختراق هاتفكم أكثر صعوبة قليلاً (أو كثيراً)

إذا سبق أن قمتم بفتح هاتفكم المقفل باستخدام التعرُّف على الوجه أو بصمة الإصبع، فإنكم تعلمون أن المقاييس الحيوية biometrics (كبصمات الأصابع وتكنولوجيا التعرف على الوجه) يمكن أن تجعل حياتكم أكثر سهولة، لا سيما عندما تكون أيديكم منشغلة أو تكونون في عجلة من أمركم. وهذه التكنولوجيا تبدو غير ذات ضرر إذا كنتم تتحكمون بوقت استخدام بيانات القياس الحيوي الخاصة بكم وكيفيته، غير أن الأمور لا تسير دائماً على هذا النحو.

في الولايات المتحدة على سبيل المثال، فإنَّ البيانات الحيوية *ليست محمية بشكل واضح بموجب القانون*، ويمكن استخدامها من قبل هيئات إنفاذ القانون للوصول إلى هاتفكم قبل أن تتاح لكم الفرصة لتلقي المشورة القانونية... بالمقابل، تجدون أن حماية هاتفكم بكلمة مرور أو رمز سري قد توفر لكم المزيد من الوقت أو الحماية.

تقوية أقفال الشاشة

بدلاً من الاعتماد على تقنية التعرف على الوجه أو مسح بصمة الإصبع، قوموا باختيار كلمة مرور أو رمز سري. يجب أن يكون الرمز الذي تعتمدونه طويلًا وفريدًا وعشوائيًا (اطلعوا على المزيد في دليل Data Detox Kit: *تقوية أقفال الشاشة*).

4. الحقائق حول بيانات الوجه

إن بيانات الوجه – مثل تلك التي يتم تجميعها من الصور الذاتية selfie والصور الموجودة على وسائل التواصل الاجتماعي – تبحث عنها بشدة هيئات إنفاذ القانون ومراقبة الحدود والوكالات الأمنية، على سبيل المثال لا الحصر. قد تساعد البيانات التي يمكن استخراجها من وجهكم تلك الهيئات على إبقائكم وجيرانكم تحت المراقبة المشددة.

قوموا بحماية خصوصيتكم

عند استخدام تقنية التعرف على الوجوه جنباً بالإضافة إلى البيانات الأخرى مثل بصمة الإصبع، والحمض النووي، والمشية، والصوت، وأنماط الحديث، فإنها تصبح أكثر دقة وفعالية. وإذا ما أُضيفت إلى المعلومات بتاريخ البحث خاصتكم، وبيانات الموقع، والأصدقاء على وسائل التواصل الاجتماعي، والسجلات العامة كالحزب السياسي وملكية الأرض، فإنه من الممكن تكوين صورة واضحة جدًا عنكم كشخص.

هل كنتم تعلمون؟ لقد تم *ربط تقنية التعرف على الوجوه بالتمييز العنصري*، إذ كثيراً ما تُخطئ البرمجية في التعرف على الأشخاص ا أصحاب البشرة الملونة، كما أوردت هذه *المقالة*.
وبسبب هذا، فقد عمد عددٌ من المدن من بينها سان فرانسيسكو و بوسطن إلى حظر استخدام الحكومة لتقنيات التعرف على الوجه. لمعرفة المزيد عن التحيز الخوارزمي، *شاهدوا هذا الفيديو*.

إنَّ الصور من حيث المبدأ تحمل الكثير من المعلومات أكثر مما تبصره العين للوهلة الأولى. قد يتوقع بعضكم شيئاً منها – مثل تاريخ ووقت التقاط الصورة ونوع الجهاز وطرازه، بيد أن في وسع المرء أيضًا أن يقوم بسهولة بتحديد الموقع استنادًا إلى إحداثيات الخريطة، وتظل هذه البيانات ملتصقة بالصور عند قيامكم بتحميلها على وسائل التواصل الاجتماعي أو مشاركتها في تطبيقات المراسلة.

لقطة الشاشة والمشاركة

للقيام بحجب بيانات الموقع من إحدى الصور بسرعة، ، يمكنكم أخذ لقطة للشاشة screenshot، بينما تتواجدون في موقع محايد، ثم القيام بمشاركة share تلك اللقطة بدلا من الصورة الأصلية. في بعض الهواتف، يمكنكم استخدام ثلاثة أصابع على الشاشة من فوق إلى أسفل لأخذ لقطةٍ للشاشة. تختلف تعليمات أخذ لقطة الشاشة بحسب طراز الهاتف، لذا قوموا بإجراء بحث على الشبكة لمعرفة كيفية القيام بذلك على هاتفكم.
للهواتف التي تستخدم نظام تشغيل أندرويد، يمكنكم كذلك تجربة أدوات التعزيز هذه لدعم خصوصيتكم: *LocationPrivacy* و *ObscuraCam*.

وإذا رغبتم في المزيد من التحديات، يمكنكم الاطلاع على *مشروع كشف المستور* Exposing the Invisible الذي أعدته تاكتيكال تِك Tactical Tech، لمعرفة المزيد عن كيفية العثور على التفاصيل المحتجبة من صورة (وهو ما يسمَّى ببيانات صيغة الملف الصوري المتبادل EXIF).

راعوا الآخرين

هل سبق أن استوقفتكم مصلحة الأشخاص الظاهرين في الخلفية عند التقاط صورة ونشرها على وسائل التواصل الاجتماعي، ؟ يمكنكم اكتساب عادة جيدة هي القيام بطمس وجوه أي أشخاص لم يوافقوا على نشر صورهم على الإنترنت.

طمس الحشود

على تطبيق *سيجنال* Signal للمراسلة، المعروف بكونه مراعياً للخصوصية، ثمة خاصية تسمح لكم بتشويش الوجوه تلقائياً في الصور التي تلتقطونها أو تقومون بتحميلها من خلال التطبيق (تعرف على المزيد عنها *هنا*).

يتضمن نظام تشغيل iOS بدوره *طريقة مختصرة لطمس الوجوه*، ولكن لا يُعرف إلا القليل جدًا عن كيفية عمل هذه الخاصية (مثلاً، ما إذا كان يتم تحميل الصورة الأصلية إلى خادم server بعيد)، الأمر الذي يجعلنا غير واثقين من التوصية بهذه الطريقة.

معلومة مهمة! قد لا تقوم تلك الأدوات بطمس بعض السمات الشخصية الأخرى كالوشوم، والملابس المتميّزة أو الشعر، وغير ذلك.

5. استخدموا برامج الدردشة بحذر

عند النظر إلى الخيارات المتاحة لكم لاستخدام تطبيقات الدردشة، فإنَّ من المهم إدراك أنها ليست متساويةً كلُّها. عليكم أن تطرحوا الأسئلة التالية:

- **هل يستخدم هذا التطبيق التشفير بين الطرفيات** end-to-end-encryption؟ ما يعنيه هذا أنه فيما عداكم والشخص الذي تتراسلون معه، فإنَّ الرسالة ستكون مُعمَّاة، ولن يكون من الممكن رؤيتها بوضوح إلا عندما يقوم أحد طرفي المراسلة بفتحها. وفي حين أن هذا قد يساعد على منع طرف ثالث من القيام بتعقُّب الرسالة، إلا أنكم ما زلتم تواجهون خطر قيام الطرف الثاني في المحادثة باطلاع شخص آخر عليها أو أخذ لقطة شاشة للمحادثة.
- **هل التطبيق مفتوح المصدر** open-source؟ البرمجيات مفتوحة المصدر تعني أن الشيفرة المصدرية لها منشورة على الإنترنت، ومتاحة بحرية لتحليلها والتعليق عليها من قبل أي شخص في العالم. وفائدة تكنولوجيا المصدر المفتوح هي أنه إذا كانت ثمة ثغرة أمنية في التعليمات البرمجية، فهناك فرصة أكبر لشخص ما للتنبُّه إليها والتحدث عنها، فيُصار بهذا إلى إصلاح المشكلة بسرعة.
- **ما الذي تقوم الشركة بجمعه وتخزينه عنكم؟** هذا اعتبارٌ شديد الأهمية، فقد تحتفظ الشركة بنسخ احتياطية من رسائلكم في خوادمها، وهذا وإن كان مؤاتيا لتمكينكم من إعادة تحميل سجل الرسائل على جهاز جديد، فإنَّه لا ينفي إمكانية قيام حكومة ما باستدعاء الشركة قضائياً لطلب سجلات الرسائل. *كلما قل مقدار البيانات التي تجمعها عنكم تطبيقات الدردشة، كلّما قلَّ ما يمكن لتلك التطبيقات أن تكشفه عنكم.*

في عام 2016، كشف الاتحاد الأمريكي للحريات المدنية ACLU أن *منشئي تطبيق المراسلة سيجنال تلقوا مذكرة استدعاء* من الحكومة طالبتهم بتسليم جميع سجلات التطبيق. ولأنهم لم يجمعوا أو يخزنوا الكثير من المعلومات منذ البدء، فإن امتثالهم لذلك الأمر لم يكن مفيداً [أي ذا نفعٍ للسلطات] على نحو استثنائي.

- **هل يتوجب عليكم الربط بين رقم هاتفكم والتطبيق؟** في حين تفرض معظم تطبيقات الدردشة متطلباً يقضي باستخدام رقم هاتفكم للتسجيل فيها، فإنَّ ثمة عدداً من تطبيقات الدردشة التي تراعي الخصوصية، وتمنحكم خيار إنشاء اسم مستخدم بدلاً من الاتصال برقم هاتفكم. تطبيق *وایر* Wire أحد الأمثلة على تلك التطبيقات.

الحفاظ على خصوصية المحادثات

استخدموا تطبيق مراسلةٍ آمناً مثل *سيجنال* أو *وایر* المشار إليهما من أجل التواصل مع أصدقائكم وأفراد عائلتكم. تجدون المزيد من الخيارات في *مركز التطبيقات البديلة* Alternative App Centre.

أنظروا إلى تطبيق الدردشة بعين فاحصة

ثمة أسئلة أخرى يتعين طرحها فيما يتعلق بأحد تطبيقات الدردشة، من مثل: هل هو في مرحلة التطوير النشط؟ ما الذي نعرفه عن الشركة؟ وكيف هو سجلها في ما يتعلق ببيانات المستخدم والخصوصية؟ هل خضعت هذه الأداة إلى التدقيق الأمني؟ من أجرى التدقيق؟ وكيف يمكنكم الإبلاغ عن الثغرات الأمنية؟

في حال كنتم ترغبون في التعمُّق أكثر، فقد جمعنا بعض المصادر النافعة التي يمكنكم الاطلاع عليها:

- مقالة أعدتها منظمة بروتِستوس Protestos: *أذاهبٌ أنت للاحتجاج؟ قم بحماية نفسك!*
- مقالة أعدتها منظمة ذا مارك أب The Markup: *كيف أُعدُّ هاتفي لاحتجاج؟*
- مقالة أعدتها منظمة ريزوم Rhizome: *مصادر رقمية لحركة مناهضة عنف الشرطة*
- مقالة أعدتها منظمة إي إف أف EFF Surveillance Self-Defense: *حضورُ احتجاج*
- شريط مصوَّر أعدته منظمة ويتنِس Witness: *كيف تصوِّر احتجاجاً*