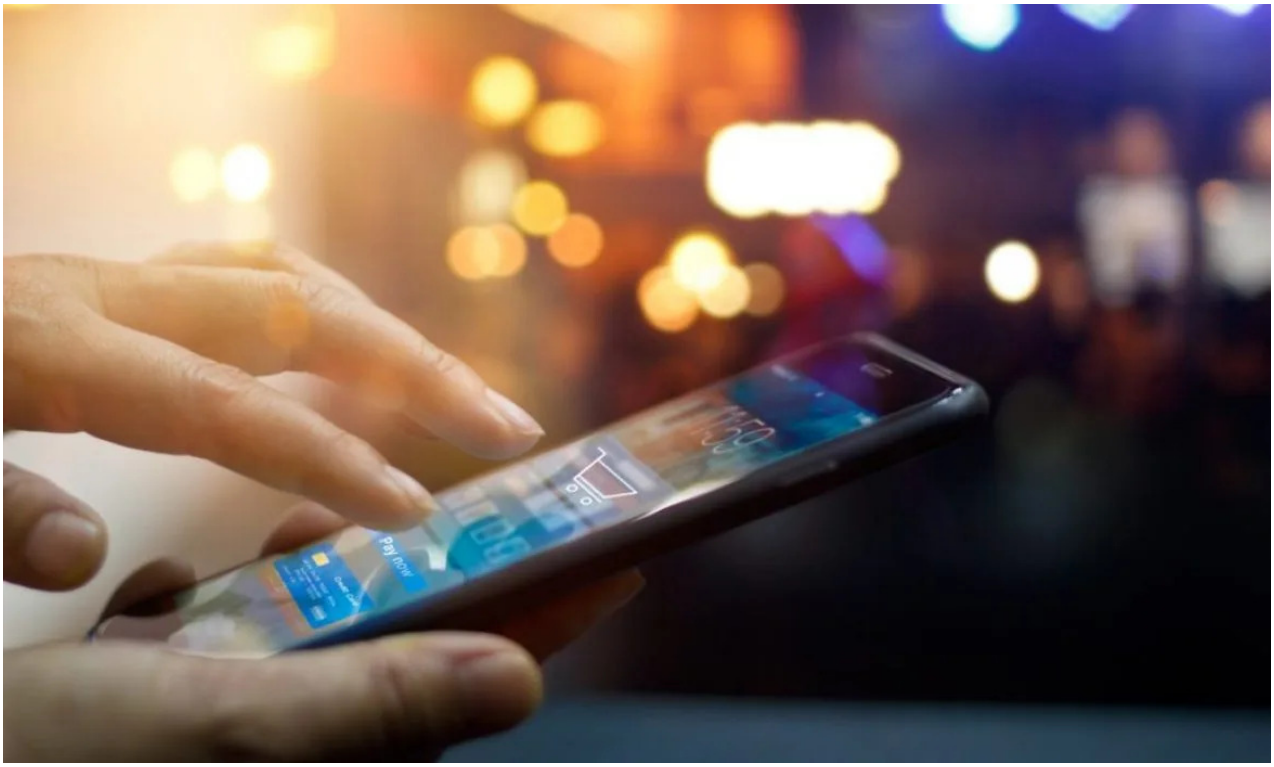
سوق المراقبة: هاتفك يخونك مع البائعين!



تخيل أن مجموعة من مطوري البرامج البسطاء، يملكون سجل بيانات يضم خريطة تحركاتك في السنوات الـ5 الأخيرة، تظهر عاداتك في التسوق والطرق التي تسلكها والأماكن التي ترتادها والأشخاص الذين تزورهم، والأهم: عنوان سكنك وعائلتك ورقم هاتفك.

معلومات قيمة كما تلاحظ، وتصبح قيمة أكثر في حال بيعها لشركات الإعلان وقاعدة البيانات، كما أنها لا تقدر بثمن في حال كنت مشتبهًا به في حادث كبير يهز البلد من نوع: اقتحام الكابيتول!

ما القصة؟

في الـ4 من فبراير/شباط 2021، دخل شخص مجهول إلى غرفة تحرير صحيفة النيويورك تايمز، يبدو أنه كان على صلة بأحد المحررين هناك، قال إن بحوزته بيانات نحو 100.000 "بيانات موقع" لآلاف الهواتف الذكية، تضم نحو 130 جهازًا داخل مبنى الكابيتول بالضبط عندما كان أنصار ترامب يقتحمون المبنى.

كان نحو 40% من الهواتف التي تم تتبعها بالقرب من منصة التجمع في "Mall National"، وفي أثناء الاقتحام، تم العثور عليها أيضًا حول مبنى الكابيتول وداخله في أثناء الحصار، وهو رابط واضح بين أولئك الذين استمعوا إلى الرئيس وحلفائه ثم ساروا بناءً عليه.

على الرغم من عدم وجود أسماء أو أرقام هواتف في البيانات، تمكن المحررون في الصحيفة من ربط عشرات الأجهزة بأصحابها، وربط المواقع المجهولة بالأسماء وعناوين المنازل والشبكات الاجتماعية وأرقام هواتف الأشخاص الحاضرين، وفي حالة واحدة، تم تعقب ثلاثة أفراد من عائلة واحدة في البيانات.

تقول الصحيفة إن المصدر شارك هذه المعلومات، جزئيًا، بسبب غضبه من أحداث 6 من يناير/كانون الثاني وكان يريد إجابات وحساب المقتحمين، لكن المصدر نفسه كان واعيًا بخطورة مشاركة هذا النوع من

البيانات السرية وتأثيرها على الخصوصية والأمن الشخصي، ليس هذا فحسب، تقول الصحيفة، وإنما لأن معظم المستهلكين لا يعرفون أن بياناتهم يتم جمعها وهي غير آمنة وعرضة لاستخدام أجهزة إنفاذ القانون وكذلك الجهات السيئة التي قد تستخدمها لإلحاق الأذى بالأبرياء.

يقول المصدر للصحيفة: "ماذا لو أردت نشرها بنفسي؟ ماذا لو كنت أريد الانتقام؟"، ويضيف "لا يوجد شيء يمنعني من فعل ذلك، إنه متاح تمامًا، إذا كان لديّ دافع لذلك، فكل ما يتطلبه الأمر هو بضع نقرات، ويمكن للجميع رؤيتها"!

فيما يتعلق بالبيانات، هناك دائمًا تلك الحجة القائلة بأن هذه البيانات يمكن استخدامها بشكل صحيح لإنفاذ القانون من خلال المحاكم وأوامر ومذكرات استدعاء، لكن الاعتقاد بأن المعلومات سُتستخدم ضد الأفراد فقط إذا خالفوا القانون أمر ساذج، إذ تُجمع مثل هذه البيانات وتظل عرضة للاستخدام وسوء المعاملة سواء اجتمع الناس لدعم تمرد أم احتجوا بحق على عنف الشرطة، كما حدث في مدن بأمريكا الصيف الماضي، فامتلاك شركات خاصة لهذه المعلومات يعتبر أمرًا خطيرًا على المستخدمين، إذا لا توجد ضمانة لعدم بيعها – عند الحاجة – في السوق السوداء.

روني فينسينت.. هل اقتحمت الكابيتول؟

تشكل حالة روني فيست مثالًا صارخًا على سهولة تقفي أثر أصحاب تلك البيانات ومعرفة تحركاتهم بأدق تفاصيلها، فمن خلال البيانات التي أرسلها المصدر إلى الصحيفة الأمريكية، استطاع فريق صحفي تتبع آثار أحد مقتحمي الكونغرس، فاستطاعوا الاستدلال على تحركاته كاملة قبل وفي أثناء وبعد حادثة اقتحام الكونغرس، ومن خلالها استطاعوا الوصول إلى عنوانه الدقيق بولاية كنتاكي "تبعد 560 ميًلا عن العاصمة واشنطن حيث يقع مبنى الكابيتول"، وبالطبع كان إيجاد حسابه على الفيسبوك سهًلا، وهناك وجد فريق التحقيق في الصحيفة صورًا منشورة له على حسابه الشخصي عن اقتحام الكونغرس.

صورة نشرتها صحيفة نيويورك تايمز لروني فيست، وهو مواطن أمريكي شارك في حادث اقتحام الكابيتول

تتبع روني فيست، لم يكن الأول ولا حتى الأصعب في استخدام تقنية "بيانات الموقع"، فقد حصلت النيويورك تايمز على بيانات تشمل 50 مليار "اتصال موقع" في العام 2019، تم استخدامها بموافقة أصحابها، لتتبع المتظاهرين من مسيرة المطالبة بحقوق المرأة عام 2017 إلى منازلهم، كما تمكنت من التعرف على الأفراد المشاركين في احتجاجات الكتلة السوداء في نفس العام، فكان من السهل متابعتهم إلى أماكن عملهم أيضًا.

في بعض الحالات – حادثة اشتباك فبراير/شباط بين مناهضي الفاشية وأنصار اليمين المتطرف في بيركلي بكاليفورنيا مثلًا – استغرق الأمر القليل من الجهد لتحديد منازل المتظاهرين ثم أفراد أسرهم.

صورة تظهر الحركة الدقيقة لأحد المحتجين

اندفاع نحو الذهب

لا يقتصر الأمر بالطبع على مراقبة تحركات المتظاهرين، إذ يفتح توافر هذه البيانات، رفقة بيانات أخرى، سوقًا كبيرًا يتيح إمكانية الوصول الدقيق لتفضيلات المستخدمين، وهي خاصية تعطي خيارات متقدمة في الإعلانات والمواسم الانتخابية.

في وثائق خاصة لشركة "phunware" وهي شركة تقنية مقرها تكساس، تقول عن السباق لجمع بيانات الموقع لاستهداف الناخبين بأنه "اندفاع نحو الذهب"، ما يشير إلى أنه "بمجرد أن تدرك الحملات

السياسية القليلة الأولى قيمة استهداف إعلانات الجوال للناخبين، سينطلق سباق حميم للوصول إليهم أوّلًا والتأثير على قراراتهم الانتخابية".

وبحسب ما أورد موقع الإنترسبت وقعت الشركة صفقة مع شركة Media Made American Consultants، وهي شركة مدير أنشأها حملة ترامب ،بارسكال براد ،لها خدمات لتقديم تقدم إذ الشركة خدمات كبيرة وتنشئ ملفًا لكل ناخب تشمل تفضيلات العمر والهوايات والميول السياسية، وبالطبع كيفية التأثير في ذلك.

يمكن للمرشحين السياسيين الحاصلين على "بيانات الموقع" دمجها مع المعلومات المالية والتفاصيل الشخصية الأخرى لبناء ملفات تعريف نفسية عميقة مصممة للتلاعب بالناخبين، ويمكن للحكام المستبدين الاستفادة من هذه المعلومات لتضليل الناخبين أو تقسيمهم ومنع الأعداء السياسيين من الظهور في صناديق الاقتراع في يوم الانتخابات.

وبعد ذلك، بمجرد وصولهم إلى السلطة، يمكنهم الاستفادة من مجموعات البيانات الخاصة بهم لتخويف النشطاء وسحق الاحتجاجات، فأولئك الشجعان بما يكفي للتمرد قد يتم تعقبهم ومتابعتهم إلى منازلهم، وعلى الأقل، يمكن وضع أسمائهم في السجلات، ويمكن للمعارضة أيضًا أن تصبح محفوفة بالمخاطر، نظرًا لأن سجل حضور الفرد في تجمع حاشد يمكن أن يتم الاحتفاظ به ضدهم في تاريخ لاحق، ويمكن أن تصبح البيانات الضخمة التي كانت ذات يوم مجالًا للمسوقين، وسيلةً لرفع الحكام المستبدين إلى السلطة ثم إحباط محاولات تنحيتهم عن الحكم.

فيما يخص العالم العربي، لا توجد معلومات تشير إلى كيفية استخدام الأجهزة القمعة لهذه البيانات، ربما لافتقار تلك البلدان للحركة السياسية أصلًا، أو لخضوع مواطنيها لرقابة من نوع آخر أو اعتماد تلك الأجهزة على نوع آخر من المراقبة، لكن الأكيد، أن وصول هذه المعلومات للمستوى التجاري، يعني بالتأكيد وصولها إلى الأجهزة الحكومية حول العالم، وإذا كانت وسائل التواصل الاجتماعي قد لعبت دورًا كبيرًا في تنظيم التجمعات خلال الربيع العربي قبل زمن من الآن، فإنها الآن وبعد عقد آخر، تشهد إمكانية أخرى لتتبع كل المشاركين في أي مظاهرات حاليّة أو مستقبلية، فالبيانات معروضة في السوق، حيث تستطيع التطبيقات الوصول إلى المكان، بمجرد موافقتك على إتاحة الوصول التي تظهر عند تحميل كثير من التطبيقات. ربما عليك التفكير مرتين قبل الضغط على زر: موافق!

رابط المقال: https://www.noonpost.com/40115/