تفاصيل صادمة.. كيف يراقبك هاتفك عندما يكون مغلقًا؟

الخميس 25 ديسمبر 2025 05:00 م

ربما لايدرك الكثير من مستخدمي الهواتف الذكية أنه يتم مراقبتهم حتى أثناء إغلاق الهاتف، مما يساعد في جمع الكثير من البيانات الشخصية عنهم، والتي يتم الاحتفاظ ببعضها لفترة وجيزة قبل التخلص منها، وبعضها الآخر يتم الاحتفاظ به على المدى الطويل. وفي كثير من الأحيان، تُستخدم لتدريب الخوارزميات.

كما يتم تداول كميات كبيرة من هذه البيانات أو يتم بيعها. وأحيانًا تُستخدم في الإعلانات الموجهة للشركات. وفي بعض الأحيان تُسلم إلى جهات حكومية مختلفة.

قد تظن أن معظم عمليات جمع البيانات لا يمكن أن تكون ضارة بشكل خاص، أو لكونها من وجهة نظرك غير مهمة، لكن عندما تُدمج مع البيانات الأخرى التي تجمعها شركات التكنولوجيا العملاقة من خلال خدماتها المختلفة، فإنها تبدأ في تكوين ملفات تعريفية مفصلة.

عند دمج هذه البيانات مع البيانات المتداولة أو المشتركة أو المشتراة من شركات أخرى، قد تكون النتائج مرعبة. تستطيع هذه الأنظمة معرفة ما تأكله، ولمن تصوّت، وما تحب مشاهدته، ومن تربطك بهم علاقات، وغير ذلك الكثير. لذلك، فإن هذا النوع من المراقبة الشاملة له تداعيات مقلقة على الأفراد.

يُعدّ تتبع الهواتف المحمولة شبكة معقدة تتضمن العديد من الآليات المعقدة وعددًا أكبر من الجهات. وعلى الرغم من صعوبة تنظيم هذه البيانات المتشابكة، فقد رتب خبراء الأمن السيبراني الجهات التي تجمع البيانات، على النحو التالي:

مزود خدمة الشبكة الخاص بك
الشركة المصنعة لهاتفك ونظام التشغيل الخاص به
التطبيقات والأطراف الثالثة
الهاكرز
الحكومة

مزودو الشبكة

توفر شركات الاتصالات البنية التحتية التي تتيح لك إجراء المكالمات وإرسال الرسائل النصية واستخدام الإنترنت، مما يمنحها رؤية شاملة لما يمر عبر هاتفك.

وتمتلك هذه الشركات سجلات لمكالماتك ورسائلك، تتضمن ما يلي:

من هو الطرف الآخر؟

وقت حدوث ذلك، ومدته (بالنسبة للمكالمات)

أي الأبراج كنت بالقرب منها

المحتوى (للرسائل النصية)

لن يقوم مزود الخدمة الخاص بك عادةً بتسجيل محتوى مكالماتك، ولكنه قد يفعل ذلك إذا تلقى طلبات من جهات إنفاذ القانون.

وفي الغالب تجمع هذه الشركات معلومات متشابهة. وأبرزها:

معلومات تصفح الإنترنت والتطبيقات

يشمل ذلك المواقع الإلكترونية التي تزورها أو تطبيقات الهاتف التي تستخدمها، سواء داخل الشبكات أو خارجها.

ويتضمن عناوين بروتوكول الإنترنت وعناوين المواقع الإلكترونية، ووحدات البكسل، وملفات تعريف الارتباط والتقنيات المشابهة، ومعرّفات مثل معرّفات الإعلانات ومعرّفات الأجهزة.

وقد يشمل أيضًا معلومات حول الوقت الذي تقضيه على المواقع الإلكترونية أو التطبيقات، والروابط أو الإعلانات التي تراها، وعبارات البحث التي تُدخلها، والعناصر الموجودة في سلال التسوق الإلكترونية الخاصة بك، وغيرها من المعلومات المشابهة.

معلومات المعدات

من الصعب معرفة ذلك من صياغة سياسة الخصوصية، ولكن هذا يشمل المعلومات المتعلقة بـ "...النوع، والمعرف، والحالة، والإعدادات، والتكوين، والبرامج أو الاستخدام".

من المفترض أن يشمل ذلك أشياء مثل رقم تعريف جهازك ونظام التشغيل واللغة وغير ذلك الكثير.

معلومات أداء الشبكة واستخدامها

يشمل هذا البيانات حول كيفية استخدامك لهاتفك عبر شبكة الشركة المزودة للخدمة.

معلومات الموقع

يتم إنشاؤها عندما تتفاعل الأجهزة أو المنتجات أو الخدمات التي تستخدمها مع أبراج الاتصالات الخلوية، وأجهزة توجيه الواي فاي، وخدمات البلوتوث، ونقاط الوصول، والأجهزة الأخرى، وأجهزة الإرسال، و/أو مع تقنيات أخرى، بما في ذلك أقمار نظام تحديد المواقع العالمي (جي بي إس). ويمكن أن تشمل هذه المعلومات موقع جهازك، وعنوانك، والرمز البريدي.

ولإكمال هذه المعلومات الكثيرة، يمتلك مزود خدمة الشبكة أيضًا معلومات حسابك وفواتيرك، بما في ذلك بيانات الاتصال الخاصة بك.

ومزود خدمة الشبكة لا يكتفي بمعرفة هويتك، ومن تتواصل معه، والمواقع التي تزورها من خلال ممارسات جمع البيانات الخاصة به، بل يُضيف إلى هذه البيانات معلومات من مصادر خارجية.

المنشورات العامة على مواقع التواصل الاجتماعي

"المعلومات الجغرافية والديموجرافية المتاحة تجاريًا". بالنسبة لمن لا يعرفون هذا المصطلح، فإن عبارة "متاحة تجاريًا" عادةً ما تكون رمزًا للمعلومات التي يمكنك شراؤها من شركات أخرى- تُعرف باسم وسطاء البيانات.

قوائم البريد التسويقية

ويشارك مزودو الشبكات البيانات أيضًا مع جهات أخرى. ومرة أخرى، قد تكون سياسات الخصوصية هذه معقدة ومكتوبة بأسلوب مبهم، إن لم يكن القصد منها تضليل الناس صراحةً، فعلى الأقل إرباكهم.

وعلى الرغم من محاولاتهم الحثيثة لتجنب التصريح بذلك، فإن مزودي خدمات الاتصالات يبيعون بياناتك، ولو جزئيًا، كما يشاركون البيانات مع الحكومة عند الطلب.

الشركة المصنعة للجهاز، ونظام التشغيل، والتطبيقات الافتراضية

إذا كنت تملك جهاز آي فون أو جوجل بيكسل، فإن الجهاز ونظام تشغيله من إنتاج نفس الشركة. أما معظم الهواتف الذكية الأخرى الشائعة، فتعتمد عادةً على نظام التشغيل أندرويد من جوجل، على أجهزة من علامات تجارية مثل سامسونج، هواوي، لينوفو، أوبو، أو غيرها.

ويعني هذه أن الهواتف مزودة ببرامج من جوجل والشركة المصنعة، وكلاهما قادر على جمع بياناتك. غالبًا ما يُنظر إلى برامج الشركة المصنعة على أنها برامج غير ضرورية ويمكن إزالتها.

على الرغم من تطوير نظام أندرويد من قِبل جوجل، إلا أنه في جوهره مفتوح المصدر. ينشر مشروع أندرويد مفتوح المصدر (AOSP) الكود البرمجي بشكل علني، ويتم تعديله لتكوين مجموعة واسعة من البرامج الأخرى. يشمل ذلك نظام التشغيل لأجهزة قراءة الكتب الإلكترونية كيندل فاير، التي ترسل بياناتها إلى أمازون، ونظام LineageOS ، وهو نسخة من أندرويد ذات تدخل محدود.

أجهزة أندرويد المزودة بخدمات جوجل للجوال

جميع هواتف أندرويد الذكية مرخصة من جوجل لتثبيت خدمات جوجل للجوال (GMS) وخدمات جوجل بلاي.

تتضمن خدمات جوجل كحد أدنى تطبيقات مثل جوجل كروم، ويوتيوب، وجوجل سيرش، وجوجل بلاي. ومع ذلك، يمكن أن تشمل الحزمة أيضًا تطبيقات شائعة أخرى مثل جيميل، وجوجل درايف، وجوجل مابس.

وفي معظم هذه الهواتف الذكية، يُضاف إلى نظام التشغيل أندرويد وخدمات جوجل برمجيات الشركة المصنعة للجهاز (باستثناء هواتف جوجل بيكسل). ستحصل الشركة المصنعة على كمية كبيرة من البيانات، لكنها تتداخل بشكل كبير مع البيانات التي تجمعها جوجل.

بينما تقدم شركات تصنيع مثل سامسونج مجموعة من تطبيقات جمع البيانات الخاصة بها، مثل بيكسبي أو سامسونج باي، إلا أن هذه التطبيقات تبدو ضئيلة مقارنة بنظام جمع البيانات الكامل لشركة جوجل.

بما أنك على الأرجح تستخدم خدمات جوجل أكثر بكثير من خدمات الشركة المصنعة لجهازك، فإنه من المفترض أن جوجل تحصل على جزء أكبر بكثير من بياناتك.

كما أن الشركة المصنعة لجهازك لديها إمكانية الوصول إليها أيضًا. وقد أثار هذا الأمر قلقًا بالغًا في الصين، حيث أظهرت الأبحاث أن شركات تصنيع الهواتف مثل شاومي وون بلس تجمع كميات هائلة من بيانات المستخدمين الحساسة، وبشكل غير متناسب من المواطنين الصينيين.

أحد الاختلافات الرئيسة بين جوجل وشركة تصنيع الهواتف هو أن الشركة المصنعة قد تبيع بياناتك، بينما جوجل من الناحية الفنية لا تفعل ذلك، .

لا تحب شركات مثل سامسونج وجوجل تقسيم سياسات الخصوصية الخاصة بها حسب المنتجات أو الخدمات الفردية، لذلك من الصعب معرفة ما يرسله كل تطبيق أو خدمة إلى خوادم الشركة بمفرده.

جمع بيانات جوجل

إذا كنت من مستخدمي أندرويد وتستخدم خدمات جوجل للجوال على جهازك، فإن أفضل طريقة لمعرفة البيانات التي تجمعها جوجل عنك هي سؤالها. يمكنك تنزيل البيانات التي جمعتها جوجل عنك من خلال لوحة تحكم حسابك على جوجل، التي تتيح لك أيضًا رؤية جميع خدماتك المرتبطة في مكان واحد.

ما لم تكن لديك مخاوف شديدة بشأن الخصوصية، فإن الملف الذي ترسله لك جوجل سيحتوي على كمية هائلة من البيانات، تغطي أشياء مثل:
سجل المواقع، بما في ذلك جميع الأماكن التي زرتها

الأنشطة داخل التطبيق

عمليات البحث على الإنترنت

مقاطع الفيديو التي شاهدتها

التطبيقات والإضافات

الإشارات المرجعية

جهات الاتصال

رسائل البريد الإلكتروني

إذا كنت تستخدم خدمات جوجل في أماكن أخرى، فلن تُعطيك هذه البيانات صورةً كاملةً لما تجمعه جوجل من خلال هاتفك فقط. وإذا كنت تستخدم بحث جوجل، أو كروم، أو خرائط جوجل، أو يوتيوب على جهاز الكمبيوتر، فستُضاف هذه البيانات أيضًا. مع ذلك، سيكون من المفيد لك معرفة ما جمعته الشركة عنك.

نظرًا لأن خدمات جوجل بلاي ومتجر بلاي أساسيان لتنزيل تطبيقات الطرف الثالث وتشغيلها، تستطيع جوجل أيضًا الوصول إلى بيانات حول تطبيقات أخرى.

وكشف تحقيق أجرته صحيفة "ذا إنفورميشن" أن جوجل لديها برنامج داخلي يُعرف باسم "أندرويد لوك بوكس"، والذي استخدمه موظفو الشركة للبحث عن كيفية تفاعل المستخدمين مع تطبيقات الطرف الثالث.

تمكن تطبيق أندرويد لوك بوكس من الوصول إلى بيانات تطبيقات أخرى عبر خدمات جوجل للجوال. وعلى الرغم من أن البيانات كانت مجهولة المصدر ولا تكشف عن هوية الأفراد، فقد ذكر موقع "ذا فيرج" أن مصادره تزعم أن جوجل استخدمت هذه البيانات "لمراقبة منافسي خدمة جيميل التابعة لها أو لمراقبة استخدام فيسبوك وإنستجرام".

كشفت دراسة أجرتها جامعة فاندربيلت عن جانب مختلف من ممارسات جوجل في جمع البيانات. فقد وجدت الدراسة أنه خلال 24 ساعة، قام هاتف أندرويد ثابت، يعمل عليه متصفح كروم فقط في الخلفية، بإرسال بيانات الموقع إلى جوجل 340 مرة. مع العلم أن الهاتف لم يكن قيد الاستخدام أصلاً.

في مرحلة أخرى من التجربة، فحص الباحثون عملية جمع البيانات في نظام أندرويد عندما تم تجنب استخدام معظم منتجات جوجل الأخرى عمدًا، باستثناء متصفح جوجل كروم. وخلال يوم من الاستخدام المعتاد، كما وصفته الدراسة، وجدوا أن جهاز أندرويد جمع موقع المستخدم حوالي 450 مرة، وأجرى 90 طلبًا في الساعة، وكان الجزء الأكبر منها موجهًا إلى مواقع إعلانية.

جمعت جوجل ما مجموعه 11.6 ميجابايت من البيانات يوميًا، وشكّلت بيانات الموقع الجغرافي والمكالمات الواردة إلى نطاقات جوجل الإعلانية حوالي ثلثي هذه البيانات. تجدر الإشارة إلى أن هذه البيانات تخص المستخدمين الذين لم يستخدموا خدمات مثل جيميل، وخرائط جوجل، ويوتيوب، وغيرها من الخدمات الشائعة. ومن المؤكد أن حجم البيانات كان سيرتفع بشكل ملحوظ لو تم استخدام هذه الخدمات أيضًا.
إ
لا أن حجم البيانات المُرسلة إلى خوادم جوجل ليس بالضرورة مؤشرًا موثوقًا لكمية البيانات الشخصية أو مدى حساسيتها.

كما كشفت الدراسة أن أجهزة أندرويد كانت ترسل عناوين ماك وأرقام إيمي والأرقام التسلسلية إلى جانب عناوين جيميل الخاصة بالمستخدمين. وأشارت الدراسة أيضاً إلى أن جوجل لديها القدرة على كشف هوية البيانات من خلال قنوات جمع البيانات المختلفة.

جمع جوجل للبيانات على أجهزة آيفون

إذا كنت تستخدم جهاز آي فون، وتستخدم في الوقت ذاته خدمات مثل كروم، ويوتيوب، وخرائط جوجل، وجيميل، فستظل جوجل تحصل على بيانات من خلال هذه التطبيقات. يمكنك التحقق من البيانات التي تجمعها جوجل من خلال جهاز آيفون الخاص بك باتباع الخطوات المذكورة في القسم السابق.

أظهرت دراسةٌ أجرتها جامعة فاندربيلت أن جهاز آي فون في وضع الخمول يرسل 0.76 ميجابايت يوميًا إلى خوادم جوجل، بمعدل أقل بقليل من طلب واحد في الساعة. وهذه الطلبات عادةً متعلقة بالإعلانات. أما عند استخدام الآي فون بشكلٍ اعتيادي، فقد وُجد أنه يرسل 1.4 ميجابايت إلى أبل يوميًا، بمعدل حوالي 18 طلبًا في الساعة.

دفعت جوجل مليارات الدولارات لشركة آبل لتكون محرك البحث الافتراضي على متصفح سفاري. وعلى الرغم من أن آبل تتمتع بسمعة أفضل بكثير في مجال حماية الخصوصية، إلا أنه لا يمكن إنكار تواطؤها في جمع بيانات مستخدميها.

أبل ونظام التشغيل آي أو إس

إذا كنت ترغب في الاطلاع على البيانات التي تجمعها آبل عنك، يمكنك تنزيلها بتسجيل الدخول إلى privacy.apple.com. اتبع التعليمات الموجودة في قسم "الحصول على نسخة من بياناتك" لتلقي نسخة منها.

مع أن هذا قد يشمل بيانات حصلت عليها آبل من مصادر خارجية، إلا أنه سيعطيك فكرة جيدة عن أنواع المعلومات التي تجمعها الشركة.
قد تتضمن هذه البيانات معلومات مثل:
معلومات حساب آبل آي دي وسجلات تسجيل الدخول.

سجل المكالمات.

البيانات المخزنة على آي كلاود.

تصفح سجل التصفح وسجلات الشراء من آب ستور وآبل بوك وآي تيونز

اشترِ الأسطوانات من متاجر بيع منتجات آبل بالتجزئة.

معلومات من تطبيقات أبل مثل مركز الألعاب، وأبل ميوزك، وآي كلاود، وتطبيق الصحة.

التطبيقات

رسميًا، يتم تنزيل التطبيقات من متجر التطبيقات أو متجر جوجل بلاي. وعادةً ما تخضع هذه التطبيقات لفحص دقيق من قبل مالكيها، وتتمتع آبل بسجل أفضل في استبعاد التطبيقات غير المرغوب فيها.

إلا أن هناك العديد من التطبيقات الشائعة تستهلك كميات هائلة من البيانات.

يمكن للتطبيقات الوصول إلى أي بيانات مُنحت لها صلاحية الوصول إليها. ستلاحظ وجود أذونات عند تجربة وظائف جديدة في تطبيقاتك، حيث ستطلب منك الإذن بالوصول إلى بيانات مثل الميكروفون والكاميرا والموقع ومساحة التخزين وغيرها. يوافق معظم المستخدمين ببساطة، إما لعدم اكتراثهم، أو لعدم فهمهم، أو لضيق وقتهم.

ولا تكتفي معظم التطبيقات بالاحتفاظ ببياناتها لنفسها فقط، بل هناك ترتيب معقد لتبادل البيانات يشمل المعلنين والعديد من الأطراف الثالثة الأخرى، بما في ذلك شركات التكنولوجيا الكبرى مثل فيسبوك وجوجل.

قد تتمكن التطبيقات أحيانًا من الوصول إلى البيانات حتى بعد تعطيل ما يبدو أنه الإذن ذو الصلة. كما يمكن للتطبيقات الخبيثة اختراق نظام الأذونات.

لذا، إذا كنت تهتم بخصوصيتك، عليك رفض منح الأذونات لأي شيء لا يؤثر على وظائف التطبيق الأساسية. وإذا طلب تطبيق ما أذونات غير منطقية، كأن يطلب تطبيق تدوين ملاحظات الوصول إلى الكاميرا دون سبب واضح، فهذه إشارة جيدة للبحث عن بديل.

تستطيع التطبيقات تتبعك من خلال معرّف الإعلانات القابل لإعادة التعيين الذي تصدره لك إما شركة آبل أو جوجل. ورغم أن هذه المعرّفات يفترض أن تكون مجهولة المصدر، إلا أنه من الممكن كشف هويتك من خلال بيانات من مصادر أخرى.

متصفح الويب

يُعدّ تطبيق التصفح، بوابتك إلى الإنترنت، من أكبر المخاطر التي تهدد خصوصيتك. إذ سيتمكن متصفحك من الوصول إلى أي بيانات أو موارد منحته الإذن بالوصول إليها. وقد يشمل ذلك بيانات حساسة مثل بيانات موقعك، والتي يمكن إرسالها باستمرار إلى خوادم الشركة على مدار اليوم.

البيانات الأكثر وضوحًا هي نشاطك على الإنترنت. يمكن للمتصفحات تتبع وتخزين تفاصيل المواقع التي تزورها يوميًا. وإذا كنت تستخدم محرك بحث تابعًا لشركة منفصلة عن متصفحك، فسترسل استعلامات البحث ونقراتك إلى مزود البحث بالإضافة إلى متصفحك. ولتقليل البيانات المُقدمة إلى جهات خارجية، يُنصح بالبحث عن متصفحات ومحركات بحث تُولي اهتمامًا أكبر للخصوصية.

إضافةً إلى ذلك، يمكن للمواقع الإلكترونية التي تزورها تتبعك أيضًا. فمن خلال تقنية بصمة المتصفح، يمكنهم معرفة الجهاز الذي تستخدمه، وإعداداته، وقد يتمكنون من تحديد هويتك. كما أن معرّفات الإعلانات من جوجل وآبل تساعدهم على تتبعك عبر الإنترنت. فتسجيل الدخول إلى حساباتك قد يترك آثارًا أثناء تصفحك للإنترنت.

ويمكن للمعلنين وشبكات الإعلان وجهات خارجية أخرى تتبعك عبر أدوات مثل أدوات تتبع جافا سكريبت وملفات تعريف الارتباط.

تطبيقات التواصل الاجتماعي والمراسلة

تورطت منصات مثل فيسبوك وإنستجرام وتويتر وتيك توك، في فضائح عديدة تتعلق بالخصوصية. ويتم معظم النشاط على هذه المنصات عبر تطبيقاتها، لذا فمن المنطقي افتراض أن معظم عمليات جمع البيانات تتم من خلالها.

يتتبع فيسبوك مواقع المستخدمين عبر التطبيق، وكان سجل تغريداتك المُحددة جغرافيًا قبل عام 2015 متاحًا في واجهة برمجة التطبيقات (API). أما إنستجرام، فيتتبع معلومات متنوعة متعلقة بالموقع، بينما يحصل تيك توك على بيانات الموقع عبر شريحة SIM وعنوان IP ونظام تحديد المواقع العالمي (جي بي إس). تمتلك هذه التطبيقات القدرة على معرفة مكان سكنك وعملك ووقت خروجك ومع من تقضي وقتك.

وتحصل هذه المنصات على أي بيانات تُقدمها لهم وتنشرها. كما تحصل على جميع المعلومات التي ينشرها أصدقاؤك عنك. وتحصل على محتوى رسائلك أيضًا، إلا إذا كنت تستخدم تشفيرًا تامًا بين الطرفين، كما هو الحال في واتساب. وحتى في هذه الحالة، لا تزال هذه الشركات قادرة على الوصول إلى البيانات الوصفية، بما في ذلك هوية المُستلم وتاريخ إرسال الرسالة.