Урок 35

Розділові знаки у складнопідрядному реченні з кількома підрядними частинами

«Як смартфон стежить за вами»

Маленькі пристрої, які кожен носить у кишені, не лише постачають своїм власникам інформацію, а й збирають її.

Наприкінці 2017 року стало відомо, що Google стежить за користувачами Android. Із початку 2017 року компанія збирала дані про місце перебування Android-пристроїв, навіть якщо на ґаджетах були вимкнені сервіси визначення геолокації. Навіть скинуті до заводських налаштувань пристрої відправляли геолокацію в Google. Тоді Google визнав, що збирає такі дані протягом майже року, але пообіцяв прибрати цю функцію. Однак виявилося, що це не єдиний підводний камінь, який чекав на користувачів.

Видання Quartz провело дослідження трьох різних телефонів на базі операційної системи Android, перевіривши, яка саме особиста інформація користувачів потрапляє на сервери Google. Хоча телефон був відключений від мережі, він передав перелік типів переміщень (відсоткове співвідношення ходьби, їзди на велосипеді та в автобусі за день) і дані вбудованого барометра, які допомагають прогнозувати погоду та точніше визначати місце перебування.

У Google стверджують, що роблять це для забезпечення кращих результатів пошуку та рекомендацій користувачам і що це особистий вибір кожного, оскільки службу місця перебування можна вимкнути. Утім, якщо це зробити, доступ до деяких застосунків може бути закрито.

А якщо не Android

Хоч iPhone вважають більш захищеним, тут також є свої причини для засмучення.

По-перше, Google збирає інформацію за допомогою всіх своїх сервісів. Тобто навіть якщо смартфон на iOS, а не на Android, проте власник користується пошуковою системою Google, уся інформація зберігається. Якщо користувач ще й використовує пошту Gmail, інформація на всіх пристроях, із яких він увійшов у пошту, синхронізується. Тобто те, що ви шукали з телефона, може раптом з'явитися як контекстна реклама на робочому комп'ютері.

По-друге, смартфони Apple також було помічено у шпигунстві. Останнього разу інженер компанії Google виявив проблему з налаштуваннями приватності в iOS, яка дозволяла програмам на iPhone вести приховану зйомку. Для цього застосунку досить було отримати від користувача дозвіл на доступ до камери, після чого він міг у будь-який час робити фото і записувати відео з фронтальної та основної камер.

Під ковпаком

Величезну кількість інформації може бути зібрано зі смартфонів незалежно від їхнього виробника як під час активного використання, так і під час роботи в фоновому режимі. Це може бути інформація про місце розташування користувача, історію пошуку в інтернеті, активність у соціальних мережах, рівень доходів і біометричні дані.

Якщо давати доступ до цієї інформації якомусь застосунку, треба пам'ятати, що він може передавати її кому заманеться. Унаслідок цього сторонні компанії можуть відстежувати, де ви перебуваєте, як швидко ви рухаєтеся і що взагалі робите.

Дуже мало програм публікують свою політику щодо конфіденційності користувачів, але навіть якщо вони це роблять, то зазвичай це довгі юридичні документи, які більшість людей не читає і не розуміє.

Авторка: Аліна Полякова,
джерело: «Економічна правда» *(скорочено та адаптовано.)*