Identifiers

- IP Address (Approx. Location)
- Internet Service Provider
- Browser Version
- Operating System and Version
- Device and size
- Which pages visited
- How you move mouse and what you click
- How long you stay on page
- Permissions (Camera, microphone, etc.)

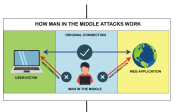
Cookies track your movements on websites and fingerprint you based on your activity

Agree to Terms & Conditions for each webpage you visit

Certificate Authorities controlled by large and obscure Private Equity Groups

CERTIFICATE AUTHORITY

Corporations sniff out SSL traffic to protect their networks from malware and unauthorized activities



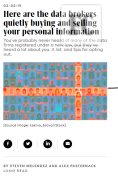
Former NPAC for 17 years

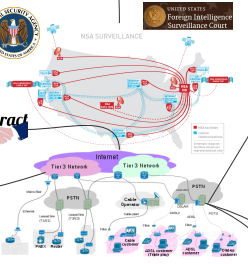
NPAC Database

- IMEI Number (Hardware identifier)
- Phone Number
- Name
- Location History
- Address
- Email
- Call & Text History

Acceptable Use Policy
Agree to Terms & Conditions with ISP

Law Enforcement access to wiretaps





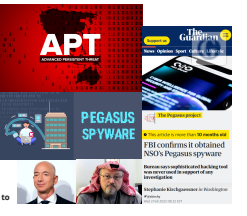
iconectiv

ERICSSON

An international mobile subscriber identity-catcher, or IMSI-catcher, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. Essentially a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack

Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About

NSO GROUP



Permissions on Device | Apps have access to

- Microphone
- Camera
- Location
- Contacts
- Emails
- Text Messages

If you use your ISPs DNS Servers, they can see what sites you visit

Apps sell your location data despite Apple policies, using simple workaround

The new data brokers: retailers, rewards apps & streaming services are selling your data

The future of the targeted ad industry depends on first party data, and your favorite retailers are open for business.

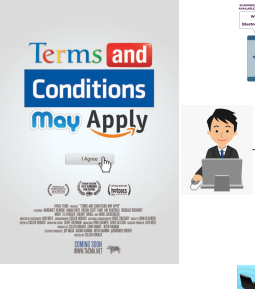
CONSUMER ALERTS
AUGUST 29, 2022

Many iOS apps sell your location data to data brokers, despite Apple's privacy policies and clampdowns, says a new report today.

Government Contractor Embedded Software in 500+ Mobile Apps to Spy on Users: *WSJ*

By Rudy Takala | Aug 7th, 2020, 5:50 pm
69 comments

Everywhere you go, you send out beacons that identify who you are based on your Wifi and Bluetooth devices and networks. Your cellular capable devices are also pinging the closest cell towers constantly identifying your location.



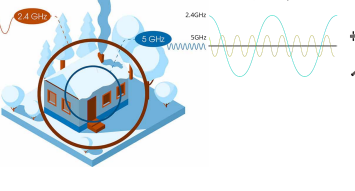
You Agree to Terms & Conditions on device

Many Wireless Routers Lack Basic Security Protections, Consumer Reports Testing Finds

Evaluations conducted with CR's new Digital Lab indicate that simple fixes could make home WiFi safer

WPS WPA
WEP WPA2

Many homeowners do not have their routers setup securely. Also many routers have vulnerabilities and old depricated hardware / software still available.



Hackers can target devices at long-range with directional antennas

Hacking Operating Systems like Kali Linux and Parrot Security come preinstalled with hacking tools making it easy to hack various networks and protocols

When it comes to being hacked, there are many different attack vectors that attackers can use to gain access to your personal information or devices. Some of the most common attack vectors include:

- **Phishing attacks:** These are attempts to trick you into giving away your personal information, such as your login credentials or financial information, by posing as a legitimate entity (e.g. your bank) in an email or message.
- **Malware:** This is software that is specifically designed to cause damage to your device or steal your personal information. Malware can be delivered through email attachments, malicious websites, or by exploiting vulnerabilities in your operating system or other software.
- **Unsecured networks:** If you connect to public Wi-Fi networks, you may be putting yourself at risk of being hacked. Unsecured networks are those that do not have password protection, so anyone can connect to them and potentially see the data you are sending or receiving.
- **Social engineering:** This is a type of attack where the attacker uses psychological manipulation to trick you into giving away your personal information or performing actions that you wouldn't normally do. For example, an attacker might call you pretending to be from your bank and ask for your account details.
- **Outdated software:** If you are using old software that is no longer supported or updated by the manufacturer, you may be putting yourself at risk of being hacked. Attackers can exploit known vulnerabilities in outdated software to gain access to your device or personal information.

To protect yourself from being hacked, it is important to be vigilant and take steps to secure your personal information and devices. This includes using strong passwords, avoiding suspicious emails and websites, keeping your software up to date, and using security tools such as antivirus software.