

Datenschützer warnen, Geräte wie Handy, Pc, TV werden über unterschwellige, unhörbare Akustik-Signale geheim vernetzt.

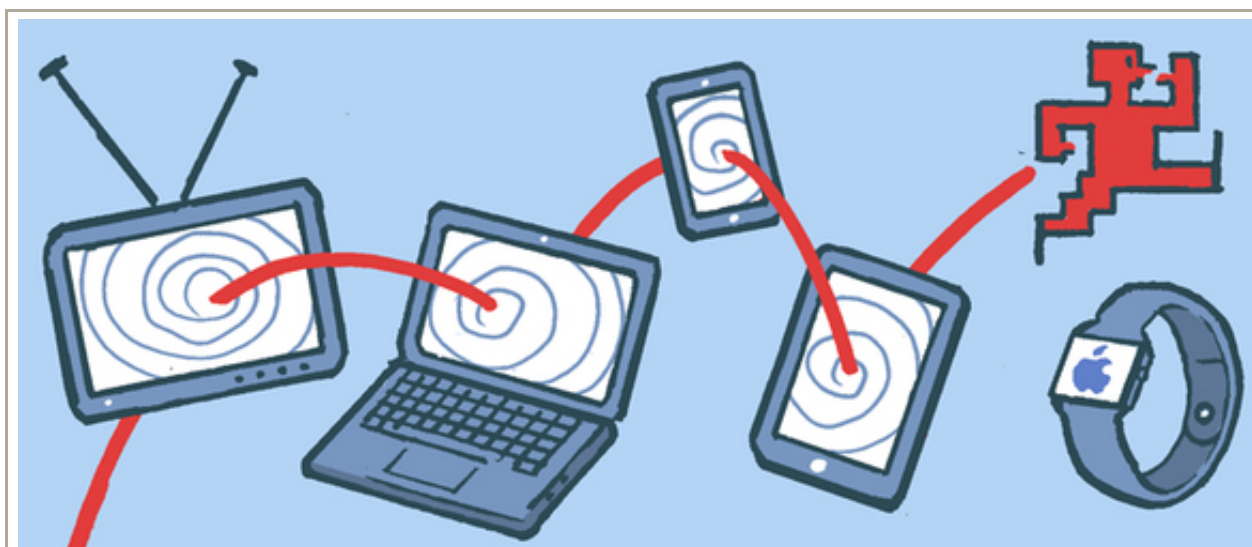
egggetsberger-info.blogspot.co.at/2015/11/datenschutzer-warnen-gerate-wie-handy.html

Wir werden immer mehr mit immer neueren Techniken ausspioniert!

Durch unterschwellige, hochfrequente Töne in Reklamesendungen können Werbefirmen nun das Verhalten von Nutzern über die Gerätegrenzen hinweg verfolgen.

Nicht ohne Grund warnen US-Datenschützer vor der neuen Technik, die auch von manchen Werbefirmen genutzt wird bzw. jederzeit genutzt werden kann. Damit können sie unbemerkt wichtige Informationen über ihre Kunden sammeln. Hintergrund: Bei dieser Technik werden TV Spots oder auch Reklame im Internet mit unhörbaren hochfrequenten Tönen hinterlegt, die für Menschen normalerweise nicht hörbar sind. Geräte können die Geräusche aber sehr wohl registrieren und auswerten, das berichtet *arstechnica-com* ([Link](#)).

Das Verfahren erlaubt es den Werbefirmen, mehrere Geräte eines Nutzers zu verknüpfen und sein Verhalten über die Gerätegrenzen hinweg aufzuzeichnen. Ein Werbespot im Fernsehen kann etwa vom Smartphone oder Tablet des Betrachters registriert werden, woraufhin seine Daten auf allen Geräten zu einem (*seinen*) Profil zusammengefasst werden können. So kann Werbung auch gezielt auf Geräte verteilt werden, eine Reklame kann Nutzer dann vom Tablet auf den Fernseher und den Computer verfolgen.



Mit geheimen, unterschwelligen, hochfrequenten Töne werden wir ausspioniert!

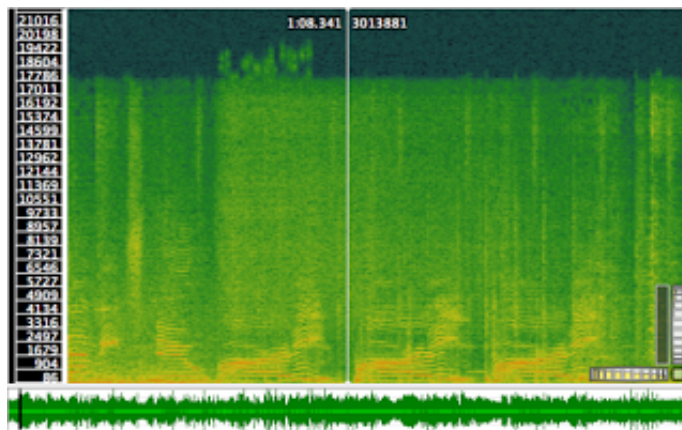
Die Firmen können laut der Kritiker so aber auch feststellen, wie lange ein Nutzer Werbung am TV sieht, welche Werbung er sich ansieht, wie oft und wie lange und ob er danach eine Websuche nach dem Produkt startet oder dieses vielleicht sogar online kauft (*Google, Microsoft, Facebook und andere machen es möglich*). Dieses **Cross-Device-Tracking** macht Datenschützern aber enorme Sorgen. In den USA befasst sich derzeit die Federal Trade Commission mit der neuen Technologie. Die größte Sorge ist, dass die vielen Geräte, die ein Mensch im Alltag verwendet, vom Fitness-Tracker über RFID-Zugangsschlüssel bis zu Handys, eine fast lückenlose Dokumentierung des Tagesablaufs ermöglichen. **Anm.:** Was Regierungen, Geheimdienste etc. sehr recht ist. Man kann so ja auch Youtube Videos und Beiträge mit unterschwelligen hochfrequenten Tönen ausstatten und auch wenn er sich so ein Video oder einen Fernsehfilm außerhalb seiner Wohnung, nicht mit seinem TV, oder seinem Computer, Handy, Tablet

angesehen hat, oder sich auch nur einen Beitrag angehört hat, weiß der "große Bruder" immer Bescheid. Man kennt dann nach kurzer Zeit noch mehr von seinen Interessen, Wünschen letztendlich von seinen Gedanken. Durch Verknüpfung von Handy-Daten, Daten über Surf-Gewohnheiten, E.Mails, Kontobewegungen u.va.m. kann man sich ein genaues Bild von der beobachteten Person machen. ...

Ein Programm mit Zukunft

Mehrere Firmen arbeiten derzeit an der Entwicklung neuer Cross-Device-Tracking-Technologien, darunter etwa Adobe, SilverPush, Drawbridge und Flurry. Besondere Sorgen macht Kritikern derzeit die Lösung von SilverPush. Die Firma versieht Werbebotschaften (*und auch anderes*) mit unterschweligen unhörbaren Tönen und platziert gleichzeitig ein Cookie im Internet-Browser. Das ausgesendete Signal wird dann von jedem Gerät empfangen, das eine App installiert hat, die das SilverPush Software-Development-Kit nutzt. Die Namen dieser **trojanischen Handy-**

Apps will das Unternehmen logischerweise nicht preisgeben, im April dieses Jahres (*April 2015*) sollen es aber bereits **67 Apps** gewesen sein -*Tendenz steigend-*, die **schon heute auf 18 Millionen Smartphones installiert sind** und die die Besitzer der Smartphones mit dieser Technologie ausspionieren. Die Firma SilverPush behauptet, dass die Software nur auf die hochfrequenten Geräusche hört, Gespräche und andere Töne aus der Umgebung würden nicht aufgezeichnet (*oder noch nicht!!!*). Eine Reihe von Marketing-Firmen soll die Technik bereits länger nutzen, ohne Wissen der betroffenen Nutzer. *Gearbeitet wird bei dieser Methode wahrscheinlich im Frequenzbereich von 17,5 und 18,5 kHz, verborgen unter den Geräuschen der Filme etc..*



Das Problem ist aus Nutzer- und Datenschützer-Sicht, dass man keine Möglichkeit hat bewusst ein Opt-Out durchzuführen bzw. gar nicht weiß, ob man schon über unterschiedliche Geräte vernetzte Daten an die Werbemacher liefert. Man darf gespannt sein, wie die Story weitergeht oder ob es der Werbeindustrie gelingt das Thema weiterhin aus dem Fokus der Aufmerksamkeit zu halten.

Dazu kommt natürlich auch die akustische Umweltverschmutzung die auch gesundheitliche Störungen mit sich bringen könnte (z.B. auch für Haustiere irritierend). Genauso ist das Ganze auch ein

Verstoß gegen das Datenschutzgesetz und ebenso höchst unethisch. Geheimdienste, Konzerne und Werber wird das alles aber nicht hindern diese Technologie zu ihren oft dunklen Zwecken einzusetzen. Doch natürlich kann man auch einfache Messgeräte (*in Richtung Ultraschall-basierte Technik*) entwickeln die dann diese unterschweligen Frequenzen auf einfache Art und Weise aufspüren und den Besitzer des Gerät vor der eingesetzten Cross-Device-Tracking-Technologien warnt.

Quellen: [arstechnica-com](http://arstechnica.com), Caschys Blog, SilverPush, u.a.

Bildquellen: (C) Div. u. SilverPush,

