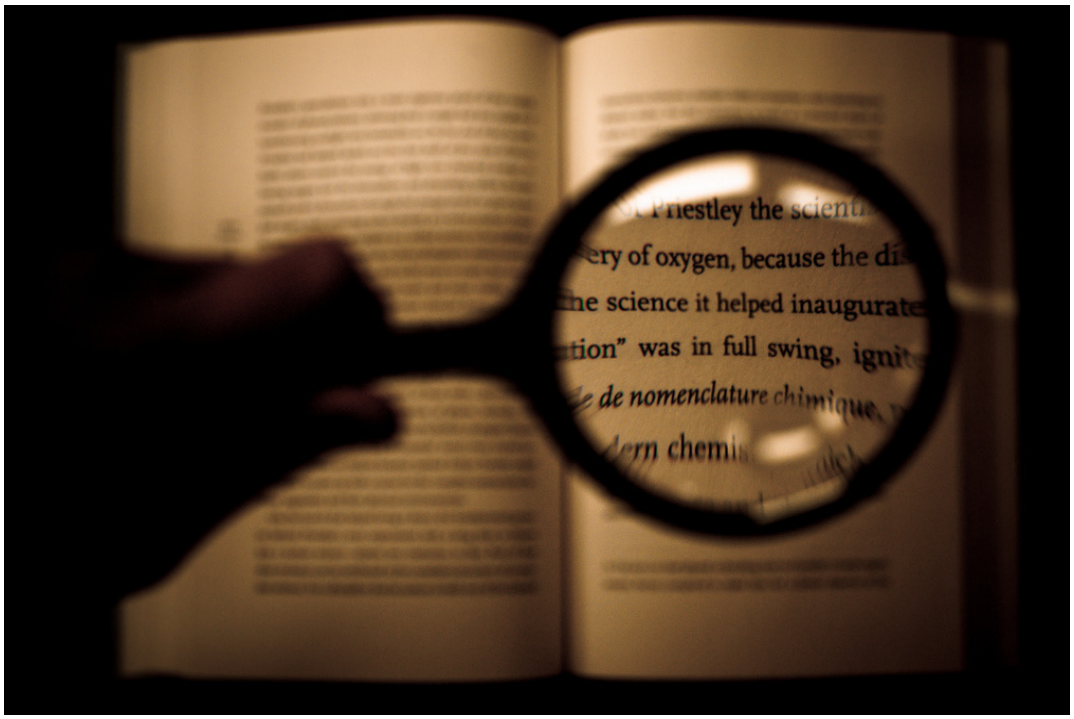
DIGITALE GESELLSCHAFT

DPI

oder

Warum wir in unseren Paketen nicht gerne herumschnüffeln lassen.



Stellen Sie sich vor, die Post öffnet alle Ihre Briefe und liest den Inhalt. Manche schreibt sie um – und andere schmeißt sie einfach weg. Das klingt absurd?

Genau das passiert mit Ihren Daten im Internet.

Was ist Deep Packet Inspection?

Im Internet werden Ihre Daten in kleine Datenpakete verpackt und darin verschickt. Jedes Paket hat einen Umschlag, auf dem Absender und Empfänger stehen. Diese Informationen sind notwendig, damit die im Internet verschickten Daten auch ankommen.

Für den Transport der Pakete reicht es vollkommen aus, nur diese Informationen auf dem Umschlag zu lesen. Aber immer mehr Provider öffnen Ihre Pakete und spionieren den Inhalt der Daten aus.

In Deutschland behindern Provider Voice over IP und Peer-To-Peer

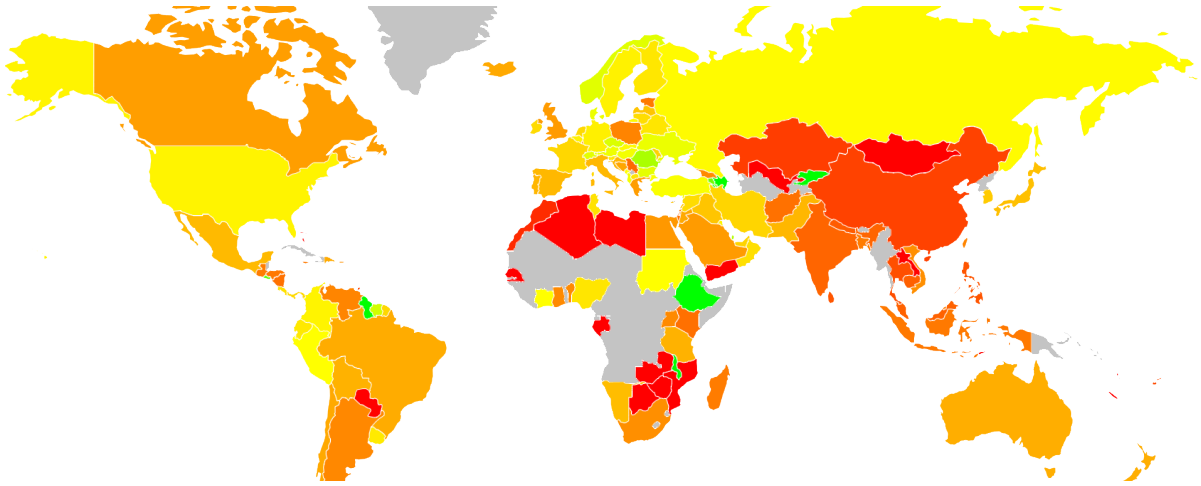
Viele Mobilfunk-Anbieter analysieren Ihren Internet-Verkehr darauf, ob Sie vielleicht Dienste von Mitbewerbern benutzen wollen, die der Provider auch kostenpflichtig anbietet. Anwendungen wie Skype oder Nachrichten-Dienste sowie offene/freie Protokolle werden dann blockiert, um stattdessen für Telefonate oder SMS viel Geld kassieren zu können.

Auch andere Anwendungen wollen die Anbieter nicht. Kabel Deutschland durchleuchtet Ihre Pakete, um zu sehen ob Sie vielleicht Filesharing betreiben. Und egal, ob Sie damit unerlaubt einen Kinofilm oder vollkommen legal Forschungsdaten austauschen: dieser Datenverkehr wird gegebenenfalls langsamer transportiert als andere Inhalte. Wenn Sie zu viele Daten in einem bestimmten Zeitraum schicken oder empfangen, wird Ihr gesamter Internetanschluss verlangsamt. Auch YouTube-Videos kommen dann nur noch in Ruckel-Qualität. Und wenn sie besonders viele Daten mit ihrer "Flatrate" empfangen oder senden, behalten sich viele Provider ein Sonderkündigungsrecht vor.

Filesharing raus, Werbung rein

Anderswo sind Provider noch einen Schritt weiter gegangen. Statt Filesharing-Verkehr "nur" zu verlangsamen, haben Anbieter wie der US-Provider Comcast gefälschte Pakete in den Internetverkehr Ihrer Kunden eingespeist, um Filesharing-Verbindungen gleich ganz abzubrechen.

In Großbritannien ließ ein Provider ohne Vorwarnung ausspionieren, welche Webseiten seine Kunden aufrufen. Aus den ermittelten Daten sollten detaillierte Interessensprofile über die Nutzer erstellt werden. Auf Basis dieser Information sollte der Datenverkehr verändert und maßgeschneiderte Werbebanner untergeschoben werden, die zum User passen sollen – und an denen der Provider verdient. Erst die EU-Kommission gebot diesem Vorhaben Einhalt.

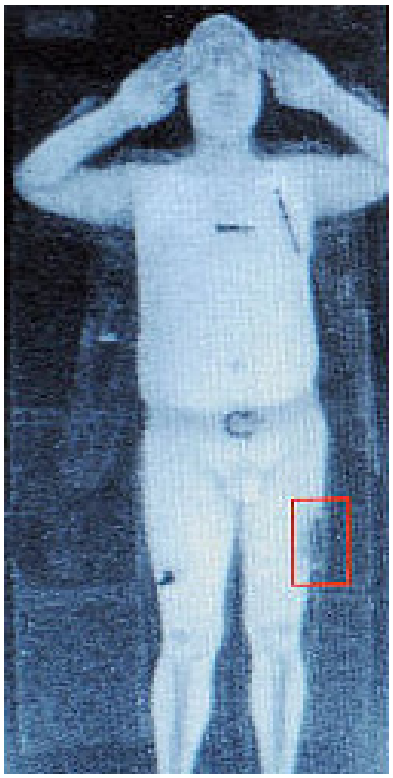


Beispiel für die Diskriminierung von Diensten:
Einschränkungen des BitTorrent-Datenverkehrs im weltweiten Vergleich.
(grün=keine Beschränkung, rot=Dienst vollständig gesperrt)

Verletzung des Datenschutzes

Das sind schwere Eingriffe in den Datenschutz und das Fernmeldegeheimnis. Welche Webseiten ein Nutzer ansurft, welche Dienste er oder sie nutzt oder welche Daten man verschickt, geht den Provider nichts an. Diese Spionage im Datenverkehr ist schon aus Datenschutzgründen unhaltbar und muss beendet werden.

Deep Packet Inspection hat aber noch weitere Gefahren, wie autoritäre Regime zeigen. Iran und China nutzen genau dieselbe Technik, um den gesamten Internetverkehr ihrer Bürger zu überwachen.



Deep Packet Inspection: Nacktscanner für ihre Daten

Zensur, Unterdrückung und Überwachung

Neben Skype und Filesharing werden dort auch Suchbegriffe und ganze Webseiten zensiert. Wer nach verbotenen Begriffen wie "Demokratie" sucht, bekommt nur eine Fehlermeldung statt dem gewünschten Inhalt.

Quasi nebenbei können alle Menschen, die zensierte Inhalte aufrufen wollen, gleich noch überwacht werden. Jede Suche, jeder Klick wird gespeichert. Wer Verschlüsselung nutzt, wird dort als verdächtig eingestuft.

Überwachungstechnologie auch in Deutschland

Die Technologie, die China dabei einsetzt, ist im Prinzip die gleiche, die auch hierzulande genutzt wird. Multifunktionale Geräte, die teilweise in Deutschland entwickelt werden, können sowohl Skype als auch Webseiten über Demokratie blockieren.

Derzeit breitet sich diese gefährliche Überwachungs- und Zensur-Technologie immer weiter aus. Wenn sie einmal großflächig installiert wurde, ist ein zensiertes Internet wie in China nicht mehr weit.

Weg mit Deep Packet Inspection

Für den Digitale Gesellschaft e. V. ist deshalb klar: Deep Packet Inspection ist eine gefährliche Technologie.

Internet-Anbieter geht der Inhalt unserer Internet-Pakete nichts an. Wenn wir nicht freiwillig zugestimmt haben, dürfen Provider in unsere Inhalte nicht hineinschauen.

Es muss – wie bei Briefpost und Telefonie – das Ende-zu-Ende-Prinzip gelten: Die Inhalte unserer Daten gehen nur Sender und Empfänger etwas an, Übermittler dürfen nur auf den Umschlag schauen.

Drosseln, Filter und Sperren stellen fuer uns einen Angriff dar, der sich direkt gegen das neutrale und offene Internet richtet, das unsere freie Gesellschaft verdient und benötigt.

Der Einsatz solcher Techniken gehört verboten, der Export in nichtdemokratische Staaten unterbunden und unter Strafe gestellt. Wir brauchen eine gesetzliche Festschreibung der Netzneutralität, um ein offenes Internet zu erhalten.

Deswegen fordert der Digitale Gesellschaft e.V.:

Echtes Netz für alle!

Mehr unter: http://echtesnetz.de

Glossar

Diskriminierung

Bezeichnet die Benachteiligung bestimmter Dienste. Da ein Provider in seinem Netzwerkmanagement entscheiden kann, welche Dienste er in welcher Geschwindigkeit weiterleitet, ist er dazu in der Lage, bestimmte Dienste absichtlich zu diskriminieren.

Netzneutralität

Grundsätzlich werden Daten im Internet gleich gut oder schlecht behandelt. Es gibt also keine Rangfolge: Keiner schaut, von wem sie kommen, keiner schaut, wohin sie gehen, keiner schaut, was für Arten von Daten es sind und keiner schaut, ob diese Daten wichtig sind. Stattdessen transportieren die Knoten und Anbieter im Internet die Daten nach bestem Wissen und Gewissen von A nach B.

Peer-to-Peer Kommunikation, P2P

Bezeichnet ein Netzwerk, in dem jeder PC auf die freigegebenen Inhalte der anderen PCs zugreifen und selbst Inhalte zur Verfügung stellen kann. Dabei gibt es keinen Server, der das Netzwerk verwaltet. So können Dateien direkt zwischen zwei oder mehreren Nutzern geteilt werden.

Voice over IP (VoIP)

Bezeichnet eine Technologie, mit der Telefongespräche über das Internet geführt werden können, die sogenante IP-Telefonie. Da es eine Vielzahl von VoIP-Anbietern gibt, die diesen Dienst kostenlos anbieten, steht VoIP in direkter Konkurrenz zu den kostenpflichtigen Gesprächstarifen der Telefonanbieter.

gefördert durch:

stiftung bridge – Bürgerrechte in der digitalen Gesellschaft

DIGITALE GESELLSCHAFT
https://digitalegesellschaft.de

Digitale Gesellschaft e.V.
Schönhauser Allee 6/7, 10119 Berlin
info@digitalegesellschaft.de | @digiges auf Twitter

Diese Broschüre wurde von Ehrenamtlichen des Digitale Gesellschaft e.V. erstellt. Die Designvorlage stammt von CtrlSPATIE.

Der **Digitale Gesellschaft e.V.** setzt sich für Bürger- und Verbraucherrechte ein. Er klärt Öffentlichkeit, Politik und Bürger, Wirtschaft und Verbraucher über die Herausforderungen der Netzpolitik auf.

Wir verzichten bewusst auf Spenden von Konzernen, um unsere Unabhängigkeit zu wahren. Dafür sind wir in unserer Arbeit auf Ihre Unterstützung angewiesen: Helfen Sie uns mit einer Spende, damit wir weiterhin unbestechlich für Grund- und Verbraucherrechte eintreten können. Nutzen Sie hierfür das Spendenformular unter digitalegesellschaft.de/spenden oder überweisen Sie Ihre Spende an:

Digitale Gesellschaft e.V., Konto-Nr: 1125012800, BLZ: 430 609 67

Spenden verwalten wir dabei transparent und offen. Wir veröffentlichen einen jährlichen Tätigkeits- und Finanzbericht darüber, wofür welche Gelder konkret verwendet werden.