

## ÜBERWACHUNGSAKTIVITÄT

In dieser Grafik können Sie erkennen, wie stark die Abfrage von personenbezogenen Daten war und ist. Es werden hier nur einige Länder dargestellt.



Schwere der Überwachung

Quelle: Enthüllungsbericht von Edward Snowden

## ANTI PRISM BÜNDNIS DER PIRATEN

Stellen Sie sich vor, Ihre persönlichen Briefe werden von Fremden gelesen, bevor sie Ihnen zugestellt werden. Genau das geschieht derzeit mit elektronischen Nachrichten, Meldungen und Gesprächen angewandt.

Die flächendeckende Überwachung durch **PRISM** und ähnliche Programmen, die auf jede verfügbare Information zugreifen, sind eine ernsthafte Gefahr für die Menschenrechte auf freie Rede und das auf Privatsphäre und damit für die Grundfesten unserer Demokratien. Zumal, wenn sie ohne Transparenz und Nachvollziehbarkeit für die Bürger angewendet werden.



<http://antiprism.eu>



Katalonien - Großbritannien und Nordirland - Spanien - Schweden - Kanada  
Weißrussland - Österreich - Deutschland - Tschechien - Griechenland  
Niederlande - Belgien - Italien - Frankreich - Tunesien - Florida (US) - Slowenien  
Luxemburg - Estland - Australien - Polen - Schweiz - Russland - Finnland



<http://antiprism.eu>

# SCHÜTZEN SIE IHRE PERSÖNLICHEN DATEN!

E-MAILS, SMS, CHATS, TELEFONATE,  
INTERNETNUTZUNG UND WEITERE  
DATENQUELLEN

## WAS IST PRISM:

**PRISM** (Akronym für „Planning Tool for Resource Integration, Synchronization, and Management“) ist ein seit 2005 existierendes und als „Top Secret“ eingestuftes Programm zur Überwachung und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten. Es wird von der US-amerikanischen National Security Agency (NSA) geführt und gehört wie andere Teilprogramme zu einem groß angelegten Überwachungsprogramm. PRISM soll eine umfassende Überwachung von Personen innerhalb und außerhalb der USA ermöglichen, die digital kommunizieren.

Wir sehen mit Bestürzung das Ausmaß, in dem die US-Regierung die Rechte europäischer Bürger und generell aller Menschen ignoriert, die US-basierte Kommunikationssysteme und Dienste nutzen. Wir sehen darüber hinaus die negativen Auswirkungen auf die Beziehungen zu den Verbündeten der USA, auf die Souveränität dieser Staaten sowie auf die Konkurrenzfähigkeit ihrer Unternehmen.

## WIR ERHEBEN DAHER DIESE 6 FORDERUNGEN:

### 1. POLITISCHES ASYL UND SCHUTZ FÜR WHISTLEBLOWER

Die US-Regierung hat schon im Fall von Bradley Manning und in anderen Fällen bewiesen, dass ihr Umgang mit Whistleblowern (Enthüllern, Skandal aufdeckern, Hinweisgebern) Anlass zu großer Besorgnis gibt (folterähnliche Methoden). Wir rufen alle Regierungen Europas auf, jedes Ersuchen um politisches Asyl oder politischen Schutz aller Whistleblower positiv und auf schnellstmöglichem Weg zu bescheiden.

### 2. ALLE FAKTEN OFFENLEGEN

Es ist inakzeptabel, dass geheime Überwachungsmöglichkeiten und -methoden die demokratischen Regeln umgehen, und so kritische und rationale Auseinandersetzungen damit verhindern, die einer Demokratie zur Abgrenzung von angemessenen gegenüber unangemessenen Vorgehensweisen notwendig sind. Wir fordern das Europäische Parlament auf, gemäß Artikel 185 seiner Geschäftsordnung einen Untersuchungsausschuss einzusetzen.

### 3. EUROPÄISCHEN DATENSCHUTZ STÄRKEN

Die derzeit verhandelte Datenschutzgrundverordnung muss verschärft werden, um einen breiten und weitreichenden Schutz von privaten und gewerblichen Daten zu gewährleisten. Lobby-Bestrebungen in die Gegenrichtung müssen abgewehrt werden. Vor allem dürfen Daten von Bürgern der Europäischen Union nicht wissentlich fremden Geheimdiensten ausgeliefert werden.

### 4. INTERNATIONALES ABKOMMEN ZUR FREIHEIT DES INTERNETS

Um sicherzustellen, dass das Internet weiterhin zur Unterstützung und Verbreitung demokratischer Grundwerte dient und nicht zur Unterdrückung demokratischer Freiheitsrechte, soll die Europäische Union ein Internationales Abkommen zur Freiheit des Internets anstreben. Darin sollte der Schutz der Vertraulichkeit von Kommunikation ebenso festgeschrieben werden wie der Schutz der Redefreiheit und des freien Zugangs zu Kommunikation im allgemeinen (und natürlich besonders im Internet) sowie einer strikten Netzneutralität (d.h. keine bevorzugte Behandlung bestimmter Seiten oder Angebote im Internet).

### 5. SOFTWARE ZUM SCHUTZ DER PRIVATSPHÄRE FÖRDERN

Als zusätzliche Möglichkeit, die Privatsphäre zu schützen, müssen Konsumentinnen und Konsumenten freie Wahl haben, Software und Dienste zu nutzen, die ihre Privatsphäre besonders schützen. Derartige Software soll Anonymität, starke Verschlüsselung auf dem gesamten Weg von Sender zu Empfänger, Peer-to-peer-Strukturen (Direktverbindung von PC zu PC), dezentrale Datenspeicherung bzw. die Möglichkeit, die Benutzerdaten selbst zu verwalten, von den Benutzerinnen und Benutzern einsehbaren Quellcode und andere Funktionalitäten zum Schutz der Privatsphäre bieten.

### 6. EIN EUROPÄISCHES PRISM VERHINDERN

Wir fordern gesetzliche Maßnahmen, um ähnliche Entwicklungen in Europa vorausschauend zu verhindern. Der direkte Zugang von Regierungsorganisationen zu Internet-Backbones (Kernbereich eines Telekommunikationsnetzwerkes), so wie er im Projekt BLARNEY durch die NSA erfolgt sein soll, muss ausdrücklich verboten werden. Solche Zugriffe ermöglichen den direkten Abgriff und die Speicherung aller Internetkommunikation ohne die Möglichkeit einer Kontrolle durch Dritte. Sie gefährden jede Kommunikation und Privatsphäre. Eine derartige unzulässige Verletzung der Integrität der Netzwerk-Infrastruktur untergräbt das Vertrauen in das Internet und alle seine positiven Aspekte.

**Mehr und ausführlichere Informationen  
finden Sie unter:**

<http://antiprism.eu>