Wir begrüßen die Tatsache, dass der derzeitige Vorschlag für das Horizon-2020-Forschungsrahmenprogramm das Ziel *„Gewährleistung der Privatsphäre und der Freiheit im Internet“* enthält. Wir rufen die Europäsche Union dazu auf sicherzustellen, dass ein **signifikant größerer Anteil** der Forschungsgelder dafür verwendet wird, die Auswahl an Software und Diensten dieser Art zu fördern, anstatt für Projekte mit dem gegenteiligen Ziel, also zur Erforschung von Überwachungsmaßnahmen und Data-Mining-Technologie, und weiters sicherzustellen, dass Projekte mit dem expliziten Ziel der wahllosen und verdachtslosen Überwachung generell abgelehnt werden.

6. EIN EUROPÄISCHES PRISM VERHINDERN

Wir schlagen legislative Maßnahmen vor, um **ähnliche Entwicklungen in Europa vorausschauend zu verhindern**.

Der **direkte Zugang** durch Regierungsorganisationen zu **Internet-Backbones**, so wie er im Projekt BLARNEY durch die NSA erfolgt sein soll, muss explizit verboten werden. Derartige Zugriffe ermöglichen den direkten Abgriff und die Speicherung aller Internetkommunikation ohne der Möglichkeit einer Kontrolle durch Dritte und kompromittieren jede Kommunikation und Privatsphäre. Eine derartige unzulässige Verletzung der Integrität der Netzwerk-Infrastruktur stellt das ganze Internet in Frage und alle seine Errungenschaften.

Wir wiederholen auch unsere Forderung nach **Aufhebung der Vorratsdatenspeicherung**. Die Verfassungsgerichte der EU-Staaten Tschechien und Rumänien haben explizit festgestellt, dass eine derartige breite, präemptive Vorratsdatenspeicherung ohne spezifische Verdachtsmomente eine grundsätzliche Verletzung der Menschenrechte darstellt. Durch die Ansammlung derartiger großer Datenmengen ohne der Zustimmung durch ein Gericht ermöglicht die Vorratsdatenspeicherung genau jene Kompetenzüberschreitungen, wie sie derzeit unter PRISM statt findet. Das stellt am Ende die Gewaltentrennnung zwischen Exekutive und Judikatur in Frage und rüttelt damit an den Grundfesten unserer demokratischen Staaten.

PETITION UNTERSCHREIBEN: http://antiprism.eu

–DIE UNTERZEICHNENDEN–

Amelia Andersdotter, MEP (Piratpartiet)

Mercè Marzo, Councilwoman Alella (Pirates de Catalunya)

Philip Pacanda, Councilman Graz (Piratenpartei Österreichs)

PIRATA.CAT – Pirates de Catalunya
PIRATE PARTY UK – Pirate Party UK
Partido Pirata
Piratpartiet
piratenpartei – Piratenpartei Österreichs
PIRATEN PARTEI – Piratenpartei Deutschland
PIRÁTSKÁ STRANA – Pirátské strany
Piratenpartij
.be – Pirate Party Belgium
PARTITO PIRATA – Partito Pirata
PARTI PIRATE – Parti Pirate
Pirate Party Florida
PIRATSKA STRANKA SLOVENIJE – Piratska stranka Slovenije
Κόμμα Πειρατών Ελλάδας
piraadipartei – Piraadipartei
Pirate Party Australia
piratepartei – Piratepartei
PIRAATTIPUOLUE – Piraattipuolue
حزب القراصنة
Polska Partia Piratów
ПИРАТСКАЯ ПАРТИЯ РОССИИ – Пиратская Партия России
Pirate Party of Canada
piratenpartei – Piratenpartei / Parti Pirate / Partito Pirata
Belurusian Pirates

Herausgeber (V.i.S.d.P)

Piratenpartei Deutschland
vertreten durch Bernd Schlömer
Pflugstraße 9a
10115 Berlin

ANTI PRISM

WIR SIND BESTÜRZT und entsetzt über das **noch nie da gewesene Ausmaß der Überwachung** von Internetbenutzerinnen und -benutzern weltweit durch PRISM und ähnliche Programme. Derartige Überwachungsmöglichkeiten, die auf jede verfügbare Information zugreifen, bedeuten eine **echte Gefahr für das Menschenrecht auf freie Rede und das auf Privatsphäre und damit für die Grundfesten unserer Demokratien**, vor allem, wenn sie ohne Transparenz und Nachvollziehbarkeit für die Wähler implementiert und exekutiert werden.

WIR SPENDEN DEM WHISTLEBLOWER EDWARD SNOWDEN BEIFALL für das, was er getan hat. Wenn ein Staat wirklich durch das Volk und für das Volk regiert wird, kann es kein Verbrechen sein, Informationen über Handlungen öffentlich zu machen, die diese Regierung im Namen des Volkes zu seinem angeblichen Schutz setzt. Eine repräsentative Demokratie beruht auf der Zustimmung ihrer Bürgerinnen und Bürger. Diese Zustimmung kann nicht erfolgen, wenn die dazu notwendigen Informationen fehlen.

Wir stellen auch mit Bestürzung das Ausmaß fest, in dem die US-Regierung die Rechte europäischer Bürger und generell die aller Menschen, die US-basierte Kommunikationssysteme und Dienste verwenden, ignoriert. Wir stellen auch den Schaden für die Beziehungen zu den Verbündeten der USA, für die Souveränität dieser Staaten sowie die Konkurrenzfähigkeit ihrer Unternehmen fest.

EUROPA MUSS sich diesen Entwicklungen energisch entgegen stemmen. In Anbetracht der Situation ist es wichtig, dass die Europäische Union hier weltweit mit einem guten Beispiel voran geht, sich als **Bewahrerin der digitalen Rechte und der Privatsphäre erweist, die geforderte Transparenz respektiert und eine Beschützerin und Fürsprecherin für Whistleblower wird**, statt weiterhin als stille Komplizin bei der Untergrabung unserer freien Gesellschaft aufzutreten.

WIR FORDERN DAHER:

1. POLITISCHES ASYL UND SCHUTZ FÜR WHISTLEBLOWER

Die US-Regierung hat schon im Fall von Bradley Manning sowie in anderen Fällen bewiesen, dass ihr Umgang mit Whistleblowern Anlass zu großer Besorgnis gibt. Die öffentliche Vorverurteilung von Edward Snowden als „Verräter“ durch eine Reihe von US-Politikern und Medien hat ein Klima geschaffen, in dem ein freies und faires Verfahren nicht sichergestellt erscheint. Im Gegenteil wird er wahrscheinlich nicht nur für seine politischen Überzeugungen zur Transparenz von Regierungen verfolgt werden, sondern es drohen auch erniedrigende und menschenunwürdige Behandlungen und Bestrafung und im schlimmsten Fall die Todesstrafe.

Wir rufen alle Regierungen Europas auf, jedwedes Ansuchen um politisches Asyl oder politischen Schutz seitens Edward Snowden sowie aller anderen zukünftigen Whistleblowern **positiv und auf schnellstmöglichem Weg** zu erledigen.

2. ALLE FAKTEN OFFENLEGEN

Es ist inakzeptabel, dass geheime Überwachungsmöglichkeiten und -methoden **die demokratischen Spielregeln umgehen**, und so kritische und rationale Auseinandersetzungen damit verhindern, welche in einer Demokratie zur Abgrenzung von angemessenen gegenüber unangemessenen Vorgehensweisen notwendig sind.

Wir fordern das Europäische Parlament auf, gemäß Artikel 185 der Geschäftsordnung einen **Untersuchungsausschuss** einzusetzen. Ergebnisse zu folgenden Fragestellungen sind zu veröffentlichen:

- Welches sind die wahren Möglichkeiten von PRISM?
- Welche Datenströme und Datenquellen nutzt es?
- Welche Verwaltungseinrichtungen der EU und ihrer Mitgliedsstaaten hatten Informationen über oder Zugang zu PRISM und gleichartigen Programmen oder zu Daten aus diesen?
- Inwiefern wurden die Charta der Grundrechte der Europäischen Union, die Datenschutzrichtlinie, die Datenschutzrichtlinie für elektronische Kommunikation oder andere EU Gesetze verletzt?

Wir erweitern diesen Aufruf auf alle nationalen Parlamente – zu untersuchen, ob nationale Verfassungen, Gesetze zum Datenschutz oder zur Spionageabwehr verletzt wurden.

3. EUROPÄISCHEN DATENSCHUTZ STÄRKEN

Die derzeit in Verhandlung stehende Datenschutzgrundverordnung müssen verstärkt werden um einen breiten und weitreichenden Schutz von privaten und gewerblichen Daten zu gewährleisten. Lobbying-Anstrengungen in die Gegenrichtung müssen abgewehrt werden.

Vor allem dürfen **Daten von Bürgern der Europäischen Union nicht wissentlich fremden Geheimdienstorganisationen ausgeliefert werden**. Artikel 42 aus dem ersten geleakten Entwurf, welcher extraterritoriale Handlungen von Drittländern wie den USA Patriot ACT und den USA Foreign Intelligence Surveillance Act behandelte und Grenzen für den Zugriff ausländischer Gerichte auf europäische Daten setzte, muss wieder eingefügt werden. Metadaten und pseudonyme Daten müssen ebenfalls geschützt werden.

Gemäß den International Safe Harbor Privacy Principles müssen US-Firmen Benutzerinnen und Benutzer informieren, wenn sie Dritten Zugriff auf ihre Daten geben. Es scheint, dass im PRISM-Programm mitwirkende Firmen diese Bestimmungen verletzt haben. In Reaktion darauf muss die EU **diese Prinzipien aufkündigen** (Kommissionsbeschluss 2000/520/EC), sodass die betroffenen Firmen unter europäische Gerichtsbarkeit fallen, sofern sie diese Handlungen nicht sofort einstellen. Safe Harbor muss dann mit effektiveren Absicherungen und Regressmechanismen neu verhandelt werden oder durch ein neues, internationales Datenschutzabkommen ersetzt werden – zum Beispiel auf den Prinzipien der Allgemeinen Datenschutz-Verordnung basierend.

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 Internet** anstreben. Darin sollte den Schutz der Vertraulichkeit von Kommunikation ebenso festgeschrieben werden wie der der Redefreiheit und des freien Zugangs zu Kommunikation im allgemeinen (und natürlich besonders im Internet) ebenso wie eine strikte Netzneutralität.

5. SOFTWARE ZUM SCHUTZ DER PRIVATSPHÄRE FÖRDERN

Als zusätzliche Möglichkeit, die Privatsphäre zu schützen, müssen Konsumentinnen und Konsumenten die Option haben, **Software und Dienste zu nutzen, welche ihre Privatsphäre besonders schützen**. Derartige Software soll Anonymität, starke Verschlüsselung auf dem gesamten Weg von Sender zu Empfänger, Peer-to-peer-Strukturen, dezentrale Datenspeicherung bzw. die Möglichkeit, die Benutzerdaten selbst zu hosten, von den Benutzerinnen und Benutzern einsehbaren Quellcode und andere Funktionalitäten zum Schutz der Privatsphäre zur Verfügung stellen.