**Geht an:** Alle Bewohner/innen dieser Liegenschaft

Betrifft: Überwachung Telekommunikation

**Datum:** 23. Juni 2016

Sehr geehrte Anwohner/innen

## Dieses Haus wird seit 18. März 2016 polizeilich überwacht.

- Sämtliche Internet-, Telefon- und Natelverbindungen der Bewohner/innen werden von den zuständigen Dienstleistern aufgezeichnet und für mindestens 6 Monate gespeichert. Der Zugriff auf diese Daten ist allen staatlichen Stellen ohne richterliche Verfügung gestattet.
- 2. Computer und Natels der Bewohner/innen dürfen jederzeit durch die Behörden mit Viren infiziert werden, um z.B. Telefon- und Skype-Gespräche abzuhören.
- 3. Eine Einsprachemöglichkeit besteht nicht.

So zumindest steht es im neuen "Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)", das am 18. März verabschiedet wurde.

Wenn Sie damit einverstanden sind, müssen Sie nichts weiter unternehmen.

Wenn nicht, oder wenn Sie auch finden, das müsste doch noch einmal öffentlich diskutiert werden, unterschreiben Sie jetzt das **Referendum gegen das neue BÜPF!** 

Den Unterschriftenbogen finden Sie umseitig, weitere Bögen zum selber Ausdrucken und Unterschreiben finden Sie auf <a href="https://www.buepf.ch">https://www.buepf.ch</a>.

Bitte bis **spätestens Montag, 27. Juni 2016** einsenden, die Referendumsfrist endet am 7. Juli! Danach ist es für lange Zeit wohl zu spät ...

Referendumskomitee BÜPF 23. Juni 2016 / rkbüpf



## Referendum gegen das Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF).

Im Bundesblatt veröffentlicht am 29.3.2016.

Name / Vornamen

(Eigenhändig, möglichst in Blockschrift)

Nr

Die unterzeichnenden stimmberechtigten Schweizer Bürgerinnen und Bürger verlangen, gestützt auf Art. 141 der Bundesverfassung und nach dem Bundesgesetz vom 17. Dezember 1976 über die politischen Rechte, Art. 59a-66, dass das Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) der Volksabstimmung unterbreitet werde.

Auf dieser Liste können nur Stimmberechtigte unterzeichnen, die in der genannten politischen Gemeinde in eidgenössischen Angelegenheiten stimmberechtigt sind. Bürgerinnen und Bürger, die das Begehren unterstützen, mögen es handschriftlich unterzeichnen.

Wer bei einer Unterschriftensammlung besticht oder sich bestechen lässt oder wer das Ergebnis einer Unterschriftensammlung für ein Referendum fälscht, macht sich strafbar nach Art. 281 beziehungsweise nach Art. 282 des Strafgesetzbuches.

Geburtsdatum

(Tag/Monat/Jahr)

Wir sagen: Nein zum Ausbau der Überwachung - Nein zum BÜPF!

## Referendumskomitee BÜPF

https://www.buepf.ch

Kanton:	PLZ:	Politische Gemeinde:	

Eigenhändige

Unterschrift

Kontrolle

(leer lassen)

2					
3					
Ablau	f der Referendumsfrist: 7.7.2016				
	nterzeichnete Amtsperson bescheinigt hie egenheiten stimmberechtigt sind und ihre			n und Unterzeichner in eidg	genössischen
Ort: _	Eigenhänd	Eigenhändige Unterschrift:		Amtsstempel:	
Datur	n: Amtliche Eigenschaft:				
an da	ste ist vollständig oder teilweise ausgefül s Referendumskomitee <b>Referendum Sto</b> ir die Stimmrechtsbescheinigung besorgt	p BÜPF, Röschibach			

In der Mitte falten, rundherum mit Klebeband schliessen und bitte sofort kostenlos an uns zurücksenden. Dankel

Wohnadresse

(Strasse und Hausnummer)

## 5 Gründe gegen mehr Überwachung durch das BÜPF!

Irreführend: Anders als behauptet, wird mit dem Gesetz die Überwachung stark ausgeweitet. Bis anhin wurde bei den Providern (an den Internet- und Mobilfunk-Zugängen) angesetzt. Nun sollen zusätzlich auch die Computer und Smartphones der Benutzer mit Hilfe von Staatstrojanern überwacht werden. Und auf der anderen Seite der Kommunikation sollen ebenfalls die Dienstanbieter die Verbindungen mit aufzeichnen. Hierzu wird der Geltungsbereich stark ausgeweitet – selbst Privatpersonen und Vereine, müssen neu Zugang zu ihrem WLAN, Mailserver etc. gewähren.

Unverhältnismässig: In der Schweiz sind bereits heute die Anbieterinnen von Post- und Telefondiensten sowie Internetzugängen verpflichtet, das Kommunikationsverhalten ihrer Kundlnnen – wer, wann, wo und mit wem kommuniziert – für sechs Monate aufzuzeichnen. Obwohl Studien nahelegen, dass diese präventive und anlasslose Vorratsdatenspeicherung nicht geeignet ist, die Aufklärungsquote zu erhöhen, soll die Speicherpflicht nun auf alle grösseren Anbieterinnen von Internetdiensten ausgeweitet werden. Diese heiklen Daten dürfen sogar im Ausland gespeichert werden.

Nicht zielführend: Viele populäre Anbieter, wie GMX oder WhatsApp, haben jedoch weder Geschäftssitz noch Infrastruktur in der Schweiz. Sie können deshalb nach wie vor nicht vom Gesetz erfasst werden. Die Ausweitung des Geltungsbereichs auf alle inländischen Personen und Firmen ist daher weder sinnvoll noch angemessen. Es ist sogar ein Standortnachteil für Schweizer Unternehmer.

Gefährlich: Mit dem Einsatz von GovWare/Trojanern soll es den Behörden erlaubt werden, in fremde Computer einzudringen und Überwachungssoftware zu installieren. Dies beeinträchtigt die Sicherheit des Systems und stellt die Integrität der Beweise infrage. Das Gesetz erlaubt den Einsatz von Spionagesoftware zudem bereits bei relativ geringen Delikten wie Diebstahl und schwerer Sachbeschädigung. Risiken und Nutzen beim Einsatz von solcher Spionagesoftware stehen in keinem Verhältnis.

Unnötig: Auch ohne GovWare/Trojaner ist es möglich, verschlüsselte Kommunikation abzuhören: Skype und andere Anbieter von Telefondiensten und Chatsoftware arbeiten auf Gerichtsbeschluss mit den Behörden zusammen. Anstatt auf gefährliche Staatstrojaner zu setzen, gilt es den (internationalen) Rechtsweg zu beschreiten.

Spenden an Stop BÜPF auf PC 61-892851-4 Unterschriftenlisten auf www.buepf.ch



Referendum Stop BÜPF Röschibachstr. 26 8037 Zürich