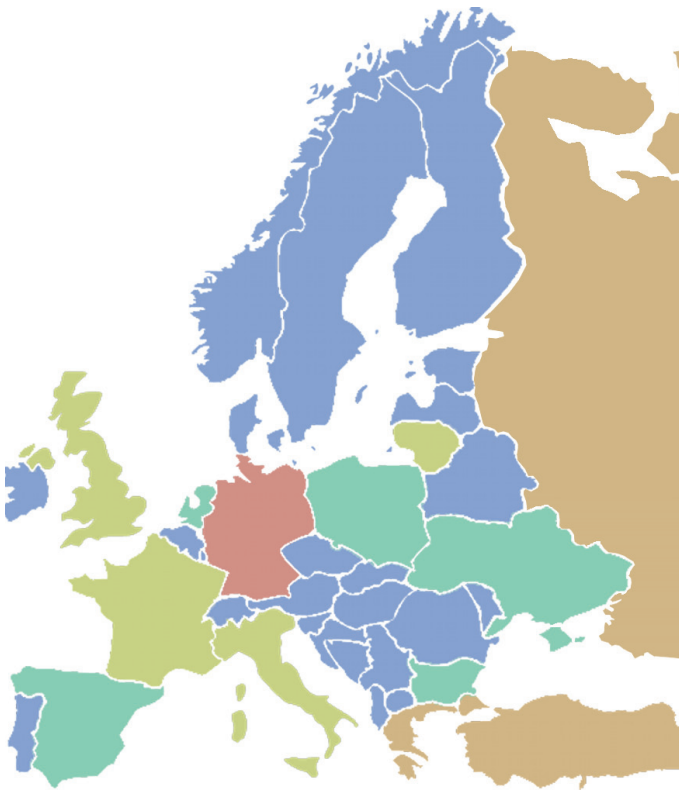
SURVEILLANCE ACTIVITY

In this graphic you can see, in which country peronsal data was collected and how often it was requested. In this view not all countries are displayed.



Severity of the surveillance

Source: Discovery report of Edward Snowden

ANTI PRISM

PIRATE (PARTY) ALLIANCE

Imagine, your personal letters were read by strangers before they reached you. Exactly this behavior is currently used for electronic mail, messages, and conversations.

Blanket surveillance capabilities such as PRISM and so many other similar programs, especially when implemented without citizens' scrutiny, seriously threaten the human rights to free speech and privacy and with them the foundations of our democracies.

http://antiprism.eu

Catalonia - United Kingdom - Spain - Sweden - Canada - Belarus
Austria - Germany - Czech Republic - Greece - Netherlands
Belgium - Italy - Frankreich - France - Florida (US) - Slovenia
Luxembourg - Estonia - Australia - Polen - Poland - Russia - Finland

http://antiprism.eu

SAVE YOUR PERSONAL DATA!

E-MAIL, SMS, CHAT, PHONE CALLS, INTERNET USAGE AND OTHER SOURCES

WHAT IS PRISM:

PRISM (Akronym for „Planning Tool for Resource Integration, Synchronization, and Management“) is a „Top Secret„ clandestine mass electronic surveillance data mining program, operated by the United States National Security Agency (NSA) since 2005. PRISM is used to allow comprehensive monitoring of people inside and outside the United States that communicate digitally.
We note with alarm the complete lack of regard the US government is showing for the rights of European citizens and, more generally, anyone who uses US-based communication services and infrastructure.
We also note the negative effect on its allies, the sovereignty of the affected countries and the competitiveness of their businesses.

THEREFORE WE CALL FOR:

1. ASYLUM AND PROTECTION FOR WHISTLEBLOWERS

The US government has demonstrated – in the cases of Bradley Manning and others – that its treatment of whistleblowers is a cause for grave concern.
We call on all governments of Europe to treat sympathetically any applications for political asylum or subsidiary protection status by whistleblowers and to speedily expedite any such applications.

2. UNCOVER THE FACTS

It is unacceptable that secret surveillance capabilities and practices circumvent democratic processes and prevent the critical, rational engagement necessary in a democracy to determine due and undue courses of action. We call on the European Parliament to form a committee of inquiry according to Article 185 of its rules of procedure.

3. STRONG EUROPEAN DATA PROTECTION

The General Data Protection Regulation currently under consideration must be strengthened to ensure a broad and far-reaching protection of private and business data. The lobbying efforts to the contrary must be resisted.

Specifically, European citizens‘ data must not knowingly be surrendered to US intelligence agencies. Article 42 from the first leaked draft proposal, which addressed extra-territorial actions by third countries such as the USA Patriot Act and the USA Foreign Intelligence Surveillance Act and imposed barriers for foreign judicial authorities to access European data, must be reintroduced.
Metadata and pseudonymous data must also be protected.

4. INTERNATIONAL TREATY ON THE FREEDOM OF THE INTERNET

To ensure that the Internet remains an empowering and democratising force rather than proceeding to be used as a tool to limit and curtail democracy and individual liberty, the EU should spearhead an international Treaty on the Freedom of the Internet.

Such a treaty should strongly protect confidentiality of communications, freedom of expression and access to information (specifically as they pertain to the Internet) as well as net neutrality (principle that Internet service providers and governments should treat all data on the Internet equally).

5. FUND PRIVACY-CONSCIOUS SOFTWARE

As an additional line of privacy defence, consumers must have the option of using software and services that strongly protect their privacy. Such software may offer anonymity, strong end-to-end encryption, peer-to-peer architectures, federation or the ability to self-host user data, user-auditable open source code and other privacy protection features.

6. PREVENT A EUROPEAN PRISM

We propose legislative measures to strengthen the defence against similar agency overreach in Europe. Direct taps by governmental agencies into backbone Internet communication channels (core part of the telecomunication net), such as the ones reportedly installed by the NSA as part of the BLARNEY programme, must be explicitly outlawed. Such taps allow storing and data-mining of all Internet communications, bypassing all other controls and procedures and compromising all confidential data and everyone‘s privacy. Breaching the integrity of the network infrastructure in this unacceptable way undermines the confidence in the entire Internet and threatens all its benefits.

By establishing the indiscriminate collection of large amounts of data without court approval, data retention programmes enable the kind of executive overreach that continues on platforms such as PRISM, threatening the separation of powers between the executive and the judiciary which is at the basis of our democracies.

More and detailed information can be found under:

http://antiprism.eu